Qualys Multi-Vector EDR

Qualys, Inc. Corporate Presentation

Welcome to this training on Qualys Multi-Vector Endpoint Detection and Response (EDR).

In this course, we will discuss how to deploy, configure and manage the Qualys EDR application and use its features to protect endpoints against malware-driven attacks, investigate events and incidents, and respond to malicious events. Further, we will also discuss how to correlate multiple vectors to mitigate the root cause of malicious events.

Training Documents

- Presentation Slide
- LAB Tutorial Supplement



Swapcard Training Event Page
(Download link at the bottom)

OR

Qualys SharePoint Server

https://bit.ly/3nyyACl

You will find the training documents for this course (lab tutorial supplement and presentation slides), below this training video (at the very bottom of the page). Alternatively, you can download the training documents for this course, from our SharePoint Server (link provided here in this slide).

Note that you will need a PDF reader like Adobe Acrobat to view these files.

Lab Tutorial Supplement

- All lab activity for this course is performed in a simulated lab environment
- Please consult the **EDR Lab Tutorial Supplement** for the following:

PLAY

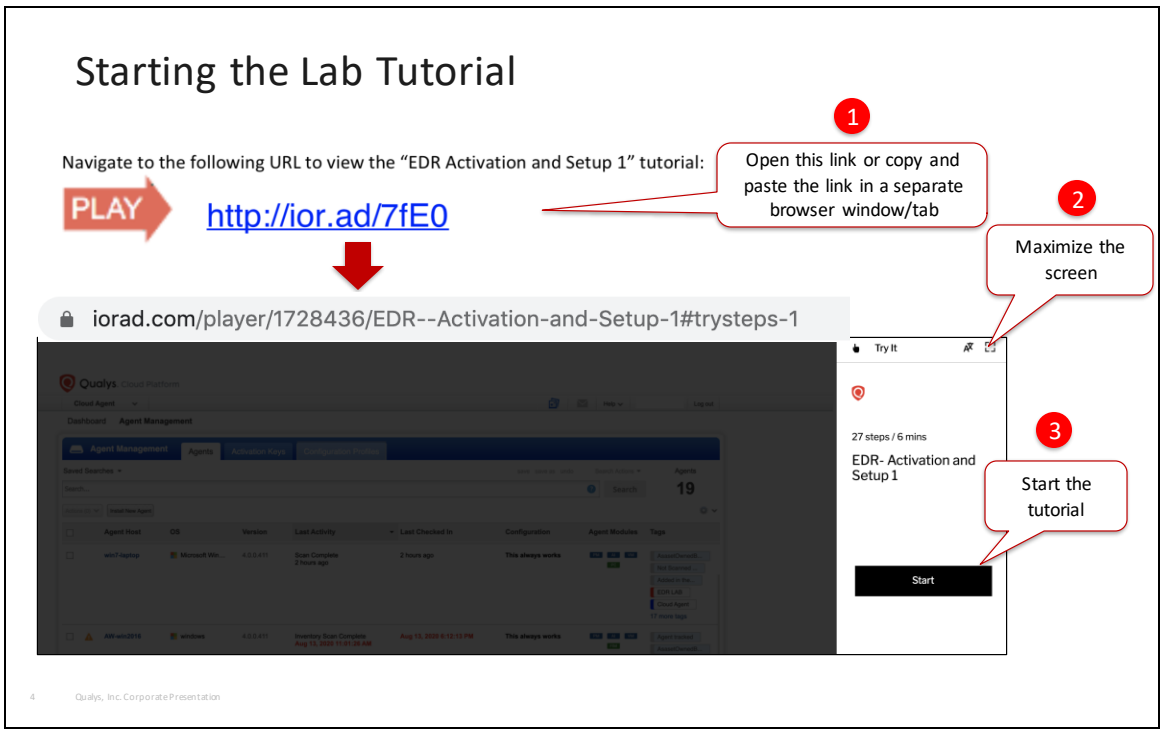
I. Link to start the lab tutorial (a separate link for each lab topic)

II. Overview of the steps performed for each topic

III. Additional supporting information

Participants will perform all lab activities for this training in a simulated lab environment.

Please consult the EDR Lab Tutorial Supplement document for further instructions.



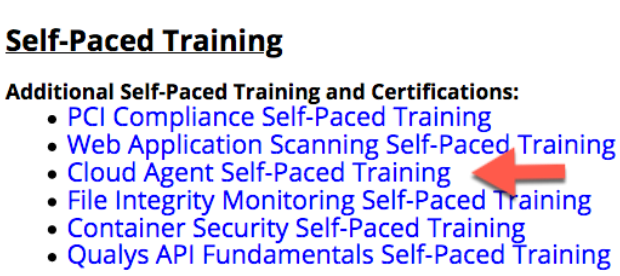
Scroll down in your Lab Tutorial Supplement to the specific topic to find the lab tutorial link. Open the link in a separate browser tab or window and start the lab tutorial.

Collapse the lab window when done and read through the lab tutorial supplement for further instructions.

Complimentary Course Recommendation

- EDR makes use of the Qualys Cloud Agent. Hence, we recommend participants enroll in Qualys Cloud Agent Self-paced course to get more information on the functioning of the agent and its deployment process:

  https://www.qualys.com/training/course/cloud-agent/


Self-Paced Training
Additional Self-Paced Training and Certifications:
PCI Compliance Self-Paced Training
Web Application Scanning Self-Paced Training
Cloud Agent Self-Paced Training
File Integrity Monitoring Self-Paced Training
Container Security Self-Paced Training
Qualys API Fundamentals Self-Paced Training

We recommend that the participants be familiar with the Cloud Agent application before taking this course. You can meet this recommendation by successfully completing the Qualys Cloud Agent training course.

Complimentary Course Recommendation

To learn the core EDR concepts and terminologies, we recommend enrolling in the Qualys EDR Foundation self-paced training course :

Foundational Courses:

Foundational courses provide background information to prepare you for taking our product-based training. If you are brand new to a particular technology, start with the foundational course. Foundational courses are shorter in length and not product-specific. When you finish the training, you will get a certificate of completion.

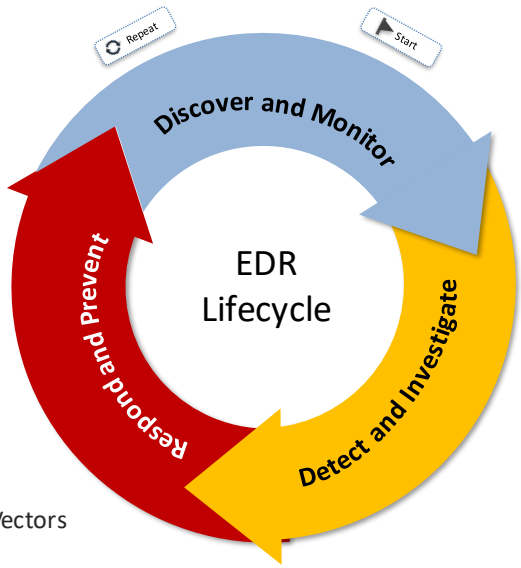
- Endpoint Detection and Response (EDR) - Foundation



We also recommend that the participants be familiar with the pertinent terms and concepts applicable to EDR technology before taking this course. You can meet this recommendation by completing the Qualys EDR - Foundation training course. This self-paced training course is available on our learning portal qualys.com/learning under the 'Foundational Courses' section.

Agenda

- ❑ **Introduction to Qualys EDR**
- ❑ **Discover and Monitor**
  - Identify Assets Missing EDR
  - EDR Activation and Setup
  - Working with the EDR Application
- ❑ **Detect and Investigate**
  - Investigate Events and Incidents
  - Hunt for Threats
- ❑ **Respond and Prevent**
  - Respond to Prioritized Events
  - Configure Rule-based Alerts
  - Correlate Prevention across Multiple Vectors



7 Qualys, Inc. Corporate Presentation

EDR is a never-ending journey because of the sheer volume of ever-changing threats with which organizations must contend. Studies show that anywhere from hundreds of thousands to a million or more new threats manifest each day. This massive volume of threats requires constant vigilance and automation around endpoint state, configuration, and behavior. That's why EDR involves a continuous, ongoing round of activity.

We'll begin this training class with an overview of the Qualys EDR application its use cases.

In the following topic, we will discuss how you can gain visibility into your IT infrastructure to identify assets where EDR needs to be deployed.

Next, we will discuss the supported platforms and the steps for deploying and configuring the EDR application.

Next, we will talk about the EDR user interface and the user roles and permissions that can be configured to manage the EDR application.

In the "Investigate Events and Incidents" topic, we will understand the event data captured by the EDR agent and the event scoring model used for threat prioritization. We will also discuss how to use Qualys Advanced Search and filter capabilities to

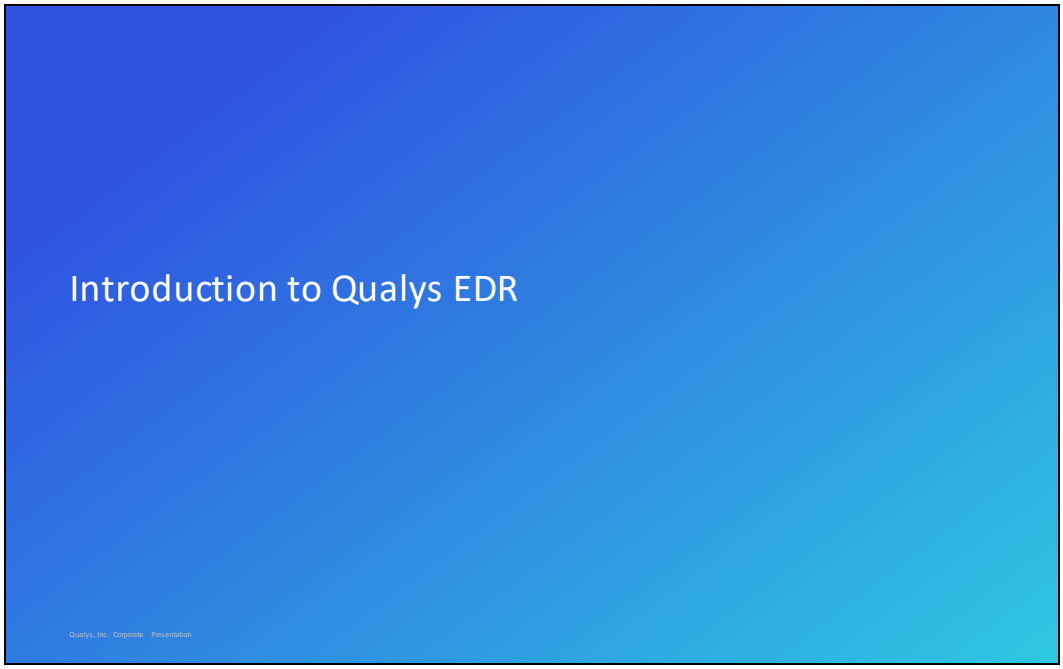
quickly find all about your incidents, events and assets in the EDR user interface.

Moving further, in the threat hunting topic, we will understand how to perform threat intel verification and find\hunt for suspicious activity using search queries and dashboard widgets.

Next, will we understand how to remediate malicious events using the EDR's multi-fold response actions.

Further, we will also discuss how to configure rule-based alerts to notify relevant stakeholders when specific events are seen in your environment.

Finally, we'll finish the course with a discussion on how you can use EDR with other Qualys applications such as Cybsersecurity Asset mgmt, VMDR, Policy Compliance and Patch Management to prevent or eliminate the root cause by correlation with additional vectors such as vulnerabilities, misconfigurations, End of Life (EOL) or End of Support (EOS) software and others.



In this topic, we'll provide an overview of the Qualys EDR application and its use cases.

Multi-Vector EDR Capabilities

Protection	▪ ***Integrated anti-malware*** proactively block known malware pre-execution ▪ ***Memory Protection*** identifies and blocks memory exploits ▪ ***Behavioral Protection*** blocks malicious activity post-execution ▪ ***Phishing Protection*** blocks access to phishing sites ▪ ***Network Protection*** blocks access to malicious URLs and IP Addresses
Detection	▪ ***Advanced Correlation Rules*** identifies suspicious/malicious activity from EDR telemetry ▪ ***Threat Intelligence*** feeds from proprietary and public sources provides real-time industry insights ▪ ***MITRE ATT&CK*** tactics and techniques provide context to attack related activities
Visibility	▪ ***Endpoint Telemetry*** captures process, file, network, and registry activity ▪ ***Timeline View*** lists the sequence of events in chronological proximity of an incident ▪ ***Process Tree visualizations*** show relationships between endpoint activity ▪ ***Identify the origins of a malware*** infection by mapping events from detection back to entry point
Response	▪ ***Threat Hunt*** for zero-day malware ▪ Seek and destroy ***Indicators of Compromise (IOC)*** ▪ ***Kill processes and quarantine files*** that passed protection layers ▪ Respond to ***Living-off-the-Land attacks***

Qualys Multi-Vector EDR includes integrated antimalware detection capabilities, providing real-time protection against the latest threats. This convergence of Malware Protection Products with Endpoint Detection & Response (EDR) is designed to deliver comprehensive protection against both known and unknown threats.

The anti-malware component protects the endpoint against all kinds of malware such as viruses, spyware, trojans and ransomware and against network attacks, and phishing.

Antivirus solutions are blind to attacks that they miss; they can't detect something that went past their defenses as they do not record the history of events. EDR offers a "Look Back" Investigation after a known breach
allowing security analysts to go back in time and investigate stored endpoint events to find the first occurrence of a breach.

EDR provides security analysts and incident responders the ability to hunt, investigate and prioritize events for remediation- by correlating event telemetry with various threat intel feeds.

You can hunt for threats through pre-built queries and MITRE detections. EDR uses the same intellectual property and query routines that professional incident response teams use to hunt for suspicious activity.

Network to endpoint correlation allows security teams to see which assets are opening, what network connections, and where these are going.

It uses a patented event scoring model to prioritize events so that responders do not have to chase every incident at the same level. And then you can remediate malicious events in real-time using the Quarantine File, Delete File, and Kill Process options.

Integrated Anti-Malware Engine



- Configure different scan options to detect and remediate malware and other threats
- Protect endpoints against attack techniques such as brute-force attacks, network exploits, and password stealers
- Enable behavioral protection to leverage machine learning models and stealth attack detection technology

10 Qualys, Inc. Corporate Presentation

The integrated anti-malware protection component includes on-access protection, which prevents new malware threats from entering the system by scanning local and network files when they are accessed, scanning boot sectors, and scanning for potentially unwanted applications (PUAs).

The On-demand scanning feature scans the file system and memory for malware and other threats and takes remediation actions.

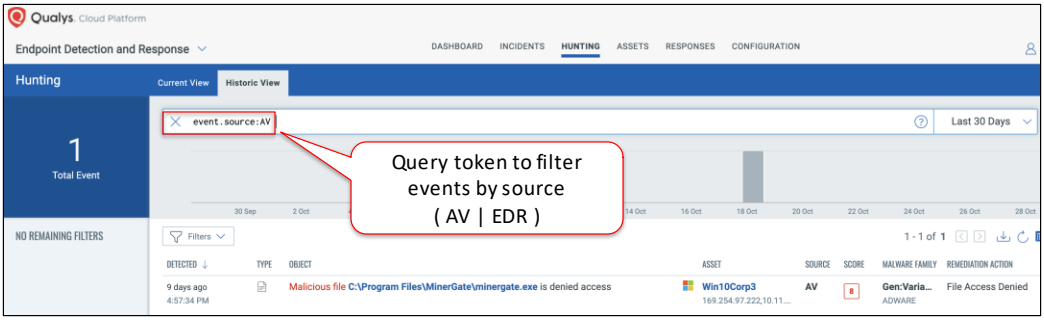
Network and Traffic Protection prevents malware from being downloaded to the endpoint by scanning incoming emails and web traffic in real-time.

In addition, it also protects against attack techniques used to gain access to specific endpoints through brute-force attacks, network exploits, and password stealers.

Phishing Protection automatically blocks known phishing web pages to prevent users from inadvertently disclosing private or confidential information to online fraudsters.

The Behavior-based protection operates on a zero-trust assumption and can monitor active applications and processes for any signs of malicious behavior. It relies on actual behavior characteristics instead of signatures or binary or code fingerprints. This allows Qualys Malware Protection to consistently detect new ransomware variants, other zero-day threats, and file-less attacks.

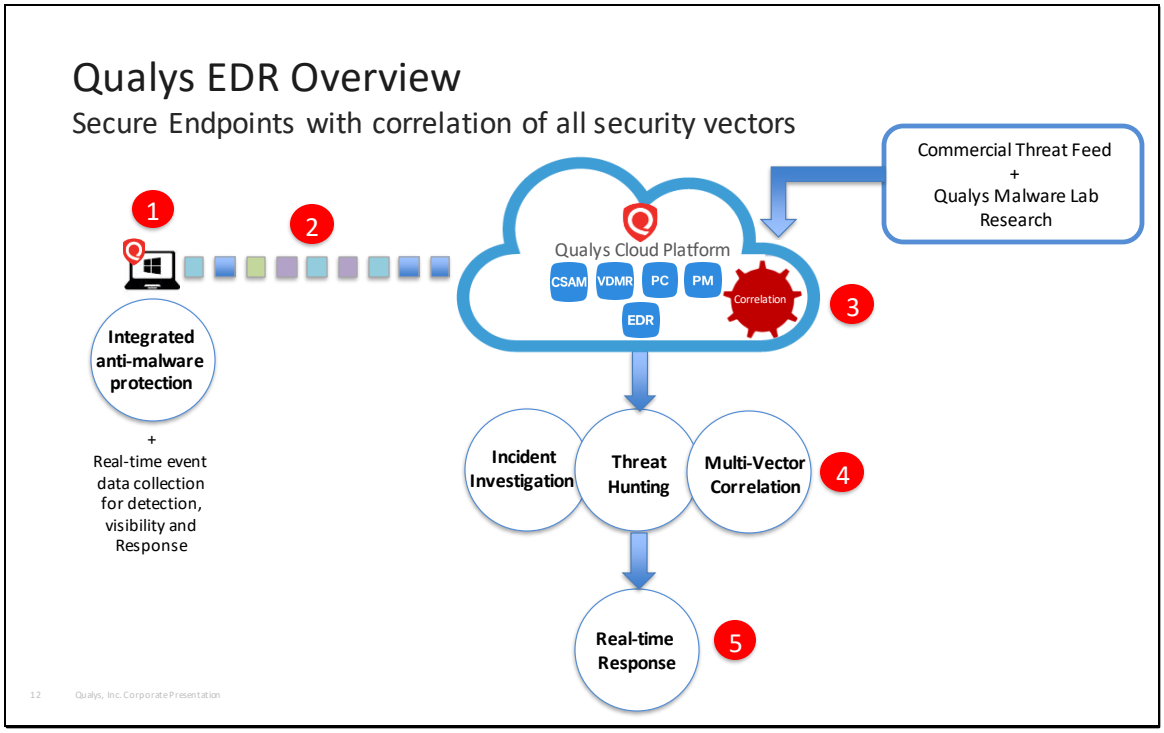
Centralized Monitoring



Details of actions taken and information about program operation are available in the Qualys cloud-based console.

Once deployed, the anti-malware component starts protecting the endpoint against all kinds of malware such as viruses, spyware, trojans, ransomware and against network attacks, and phishing.
And Details of actions taken and information about program operation are available in the Qualys cloud-based console.

Malware detection events can be viewed and analyzed from the EDR application, allowing users to enrich malicious events with contextual events collected by Qualys EDR.



Now let's talk about how our EDR solution works.
This is delivered through the Cloud Agent, enabling protection for the endpoint through the integrated anti-malware engine and continuous monitoring and data collection through the EDR Manifest.

The agent collects and sends data endpoint telemetry data in real-time to the Qualys cloud platform.
This event data is natively correlated with threat intelligence and research from Qualys Malware Labs. Events are prioritized using a patented scoring system allowing for a prioritized response.

And then you can view all malicious events, infected hosts and investigate incidents using system events and details captured by the cloud agent in the EDR application.

EDR expands the capabilities of the Qualys Cloud Platform to deliver threat hunting and remediation response. EDR detects suspicious activity, confirms the presence of known and unknown malware, and provides remediation response for your assets.

Lastly, EDR unifies different context vectors like asset discovery, rich normalized software inventory, end-of-life or end-of-support visibility, vulnerabilities and exploits, misconfiguration, in-depth endpoint telemetry, and network reachability with a powerful backend to correlate it all for accurate assessment, detection and response

all, in a single, cloud-based app.

Correlation with all attack vectors helps eliminate the root cause and minimize the possibility of similar attacks in the future.

Qualys Malware Labs



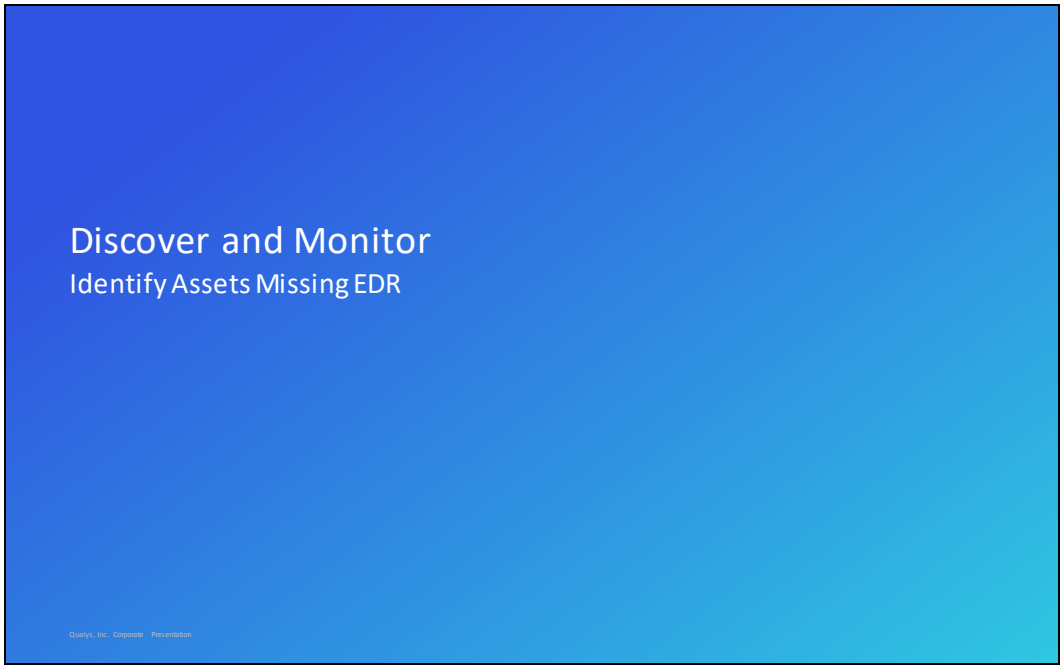
Malware research team

- Develops **static signatures** and **behavior models** to detect malware based on how malware installs and executes
- **Family-based detection** of known/unknown variants zbot, Keybase, Backoff, GlassRAT, …
- Categorize **enterprise-targeted malware** such as financial, keylogger, Point of Sale (POS), Remote Access Trojans (RAT), …

Qualys EDR uses various threat intelligence sources for automated threat detection and validation. EDR also leverages research from Qualys Malware Labs to provide accurate malware detection with few false positives.
Qualys Malware Labs team is based on the years of vulnerability and exploit research to support EDR.

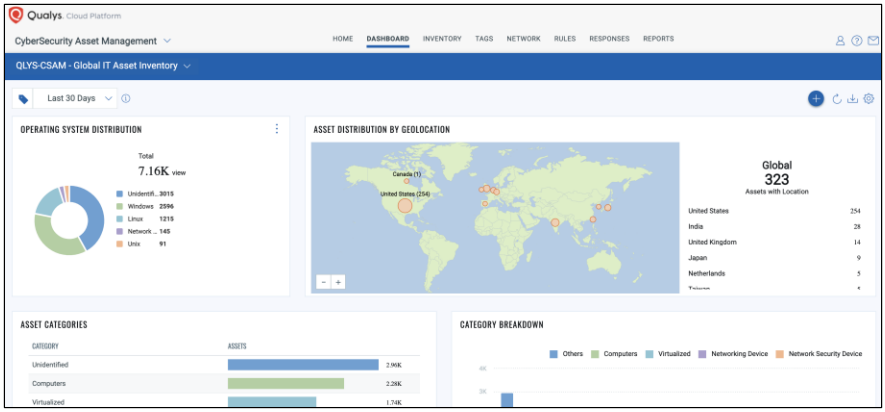
EDR focus is specifically on enterprise-targeted malware families where malware authors use automation to create different variants of existing malware families to avoid detection by signature-based systems.

Our approach uses both static signatures and behavior models that looks at how these malware variants persist, execute, and communicate.



In this topic, we'll examine the supported platforms and steps for activating and setting up Qualys EDR.

Start with Visibility



- CSAM provides complete visibility into the entire hybrid IT infrastructure
- Helps eliminate blind spots
- Provides vital context needed for a multi-vector EDR approach

15 Qualys, Inc. Corporate Presentation

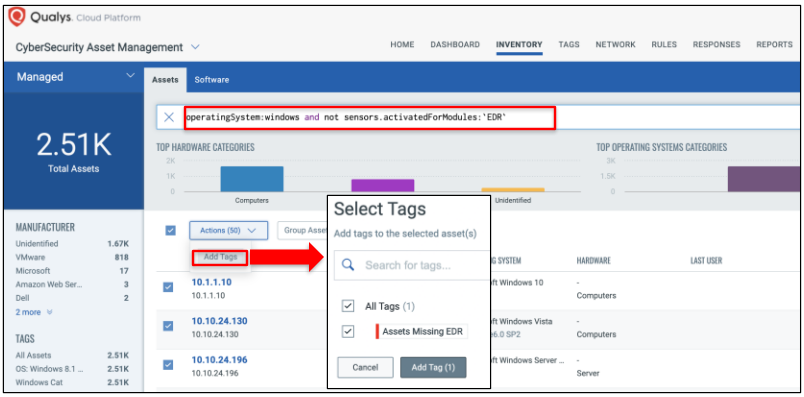
Endpoint security starts with visibility.

Qualys CyberSecurity Asset Management (CSAM) provides you a single source of truth for your assets. It's a central location where you can view the data collected from different sensors you've deployed. That data is then normalized and categorized to understand it better and group it in many ways. Because you're getting an inventory, you are completing the first step of the security and compliance teams which is visibility.

Qualys EDR works with Qualys CyberSecurity Asset Management (CSAM) and hybrid sensors to gain visibility across the infrastructure - tells what endpoints, servers, technologies you have in environment. This provides vital context needed for endpoint security and let's you know exactly where EDR can be deployed for eliminating blind spots.

Eliminate Blind Spots

- Quickly identify assets missing Cloud Agents and EDR
- Leverage Asset Tagging for easy identification
- Create widgets to dynamically track assets without EDR



CSAM supports the use of elastic queries, which helps you quickly identify assets from your infrastructure missing EDR capability.

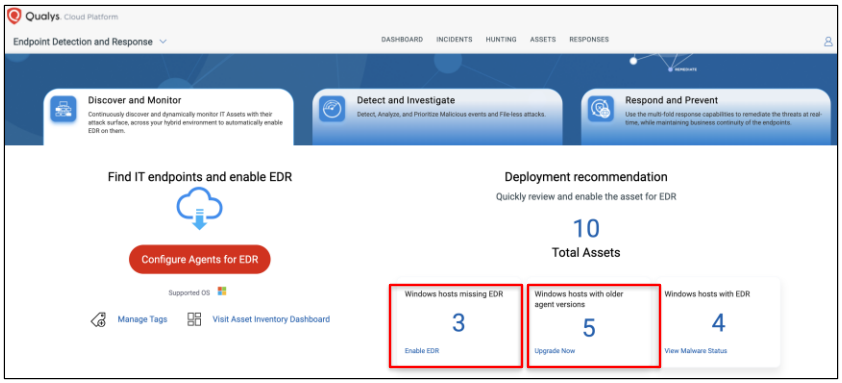
You can run the following search query from the "Assets" tab under the "Inventory" section in CSAM to identify Windows assets that do not yet have EDR on them:

```
operatingSystem:Windows and not
sensors.activatedForModules:EDR
```

And you can leverage the same search queries to create dashboard widgets to dynamically track such endpoints that should have EDR but are missing it.

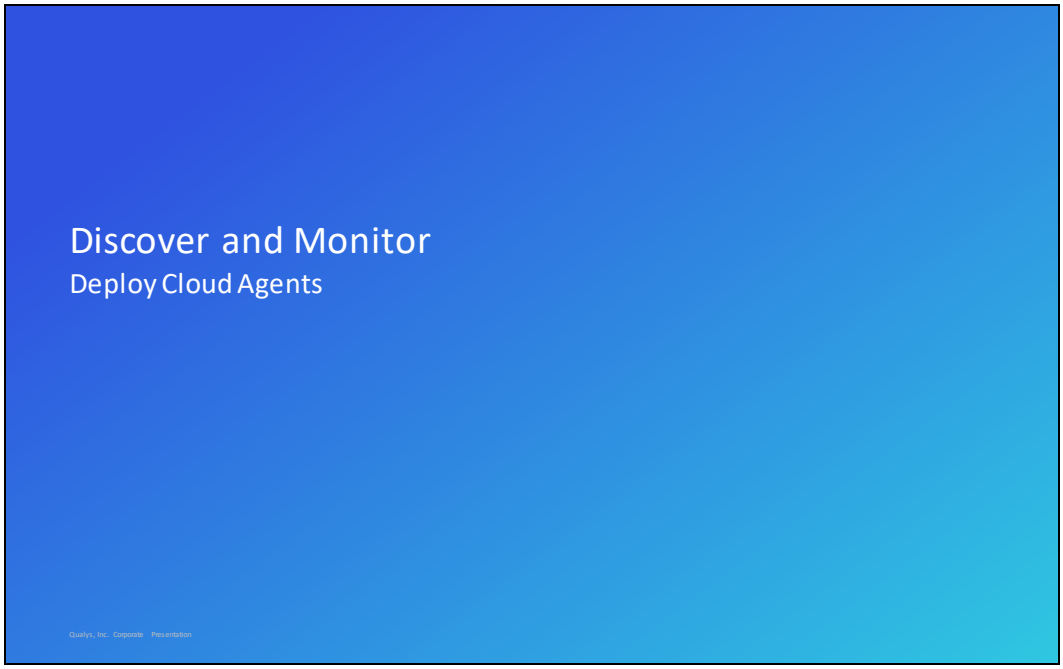
You can then tag such assets, deploy Cloud Agents, and activate EDR on them.

Identify Cloud Agent Hosts without EDR


Qualys Cloud Platform
Endpoint Detection and Response
DASHBOARD
INCIDENTS
HUNTING
ASSETS
RESPONSES
Discover and Monitor
Continuously discover and dynamically monitor IT Assets with their attack surface, across your hybrid environment to automatically enable EDR on them.
Detect and Investigate
Detect, Analyze, and Prioritize Malicious events and File-less attacks.
Respond and Prevent
Use the multi-fold response capabilities to remediate the threats at real-time, while maintaining business continuity of the endpoints.
Find IT endpoints and enable EDR
Configure Agents for EDR
Supported OS
Manage Tags
Visit Asset Inventory Dashboard
Deployment recommendation
Quickly review and enable the asset for EDR
10
Total Assets
Windows hosts missing EDR
3
Enable EDR
Windows hosts with older agent versions
5
Upgrade Now
Windows hosts with EDR
4
View Malware Status

- Identify Cloud Agent hosts missing EDR
- Identify hosts running older Cloud Agent versions *(CA version < 4.1)*

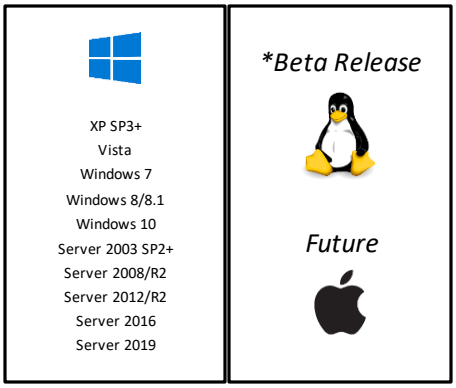
The “Windows hosts missing EDR” widget identifies agent hosts that do not have EDR enabled and the “Windows hosts with older agent versions” widget identifies hosts running Cloud Agent version lower than 4.0.0.



In this topic, we'll examine the supported platforms and steps for activating and setting up Qualys EDR.

Supported OS Technologies

Current Support



Cloud Agent Platform Availability Matrix

Windows | Linux | Linux arm_64 | IBM AIX | Apple MacOS

Qualys certifies the two latest Agent releases for new operating systems and their updates. While not explicitly certified, all Agent versions that are not End-of-Service should also support these operating systems.

Windows

Current Release: 4.4

End-of-Service versions: See Appendix

Supported Platforms				Supported Qualys Modules/Agent Versions				
Vendor	Operating System	Arch	Installer	Inventory / VM	PC	PC UDC	SCA	EDR
Microsoft	Windows XP SP 3+ Vista	x86_64 x86_32	(.exe) beta (.msi)	4.4, 4.2	4.4, 4.2	4.4, 4.2	4.4, 4.2	4.4, 4.2 (excluding XP)
Microsoft	Windows Embedded 7	x86_64 x86_32	(.exe) beta (.msi)	4.4, 4.2	4.4, 4.2	4.4, 4.2	4.4, 4.2	4.4, 4.2
Microsoft	Windows 7 Windows 8/8.1	x86_64 x86_32	(.exe) beta	4.4, 4.2	4.4, 4.2	4.4, 4.2	4.4, 4.2	4.4, 4.2

* Please contact your Qualys TAM to enroll in the EDR for Linux beta program

https://www.qualys.com/docs/qualys-cloud-agent-getting-started-guide.pdf

19 Qualys, Inc. Corporate Presentation

Qualys EDR relies on Cloud Agent for collecting event telemetry data and for responding to malicious events.

Presently, the Qualys EDR module is available for Windows-based operating systems.

The EDR Linux agent is available in beta release for select Linux distributions. We recommend that you reach out to your Qualys TAM for more information on enrolling for the EDR Linux Beta program.

And additional OS support is “on-the-way” for MacOS.

For the latest supported operating systems for EDR, see Cloud Agent Platform Availability Matrix in the **Cloud Agent Getting Started Guide**.

Deployment Requirements

- EDR performs active monitoring and data collection from endpoints in real-time
- Has specific system requirements for hardware and software compatibility

Qualys recommends carrying out EDR onboarding activities with the support of your TAM

https://www.qualys.com/docs/qualys-edr-onboarding-guide.pdf

Given the nature of data collection requirements for the EDR solution, Qualys has put together a set of recommendations to help you onboard the EDR product.
Please consult the EDR onboarding guide for more details.

Getting started with EDR



Follow these steps to run EDR on the target host:

1. Install Cloud Agent with EDR

   OR

   Activate EDR on agent host (for existing agents)

   **Cloud Agent version 4.1 and above required to have support full EDR functionality (real-time event data collection and response actions)*

2. Assign target agent host to a Configuration Profile that has EDR enabled

Although EDR is supported as a separate application, it is an extension of the Qualys Cloud Agent (CA) application.

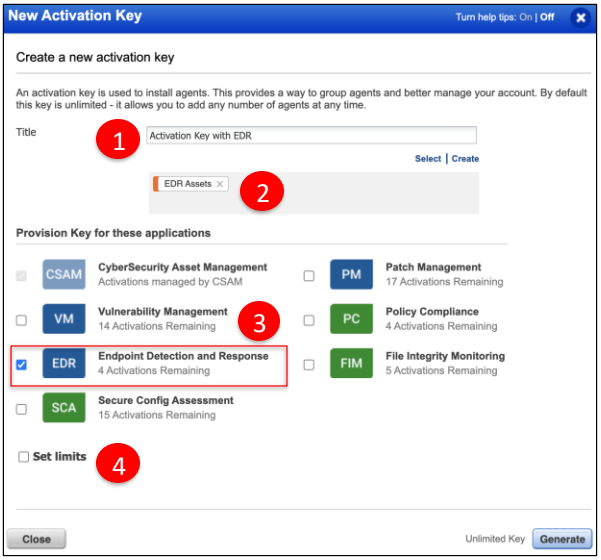
So, installing the CA is the first step to using EDR. Note that full EDR functionality (including response actions and real-time windows event data collection) is only available for Cloud Agent version 4.1 and above.
Please consult the Cloud Agent training module for instructions on installing the Cloud Agent on a Windows host.

Three options are provided for activating the EDR module from within the CA application:
1. Agent Activation Key
2. Host "Quick Actions" Menu
3. CA Application Program Interface (API)

Agent host assets must use a Configuration Profile that is configured for EDR. The EDR configuration options within the Configuration Profile provide settings to configure payload size, the time lapse between payload transfers and disk space allocation on the asset for caching EDR data.

Agent Activation Key

1. Activation Keys allow you to manage and control the distribution of Cloud Agents.
2. Add a ”static” tag to each key to label and track agent hosts deployed.
3. Application modules selected will be activated at agent deployment.
4. Create keys without limits or set limits by the maximum number of agents or expiration date.



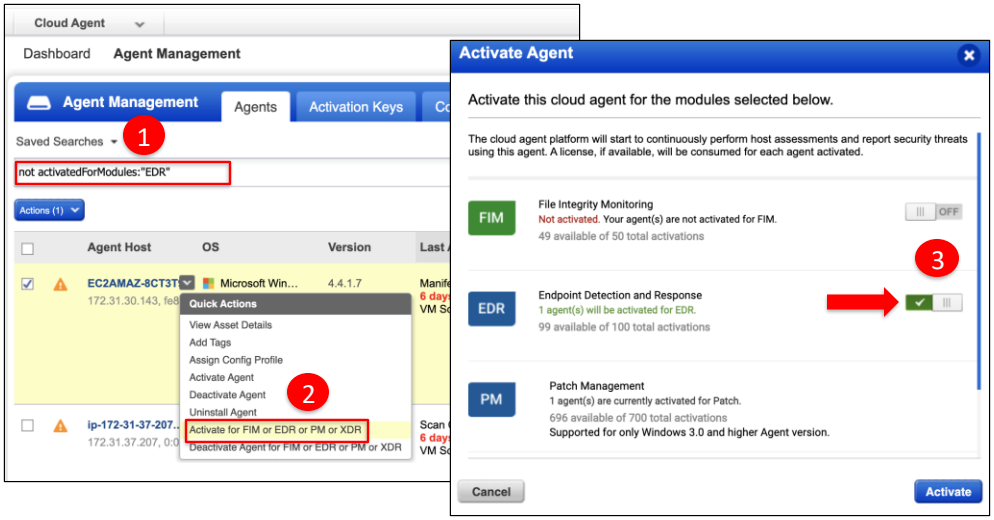
Activations Keys contain the components to deploy agents successfully. You must first create one or more Activation Keys, before installing an agent.

Qualys recommends adding a ”static” tag to an Activation Key, to easily identify the assets it deploys.

Any application module selected in the key will be activated at the time of deployment. Application modules not selected can always be activated later (after deployment).

Options are available to limit the number of agents deployed with any key.

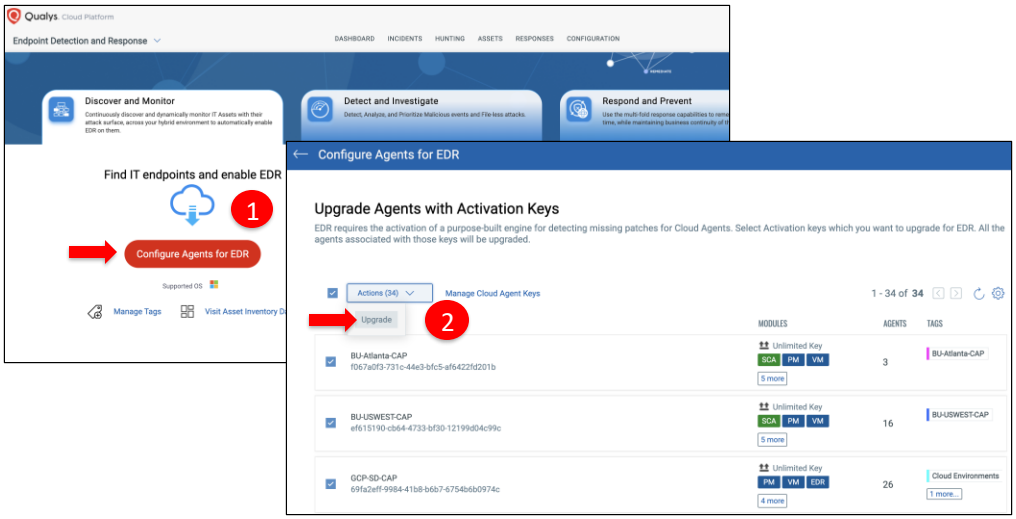
Host “Quick Actions” Menu



You also have the option of activating the EDR module from the installed agent’s quick action menu within the CA user interface. This way you can activate EDR for an individual host or for multiple hosts in bulk.

Alternately, you can activate EDR in bulk using the CA Application Program Interface (API). Please consult the CA API guide for more information.

Upgrade Multiple Agent Activation Keys



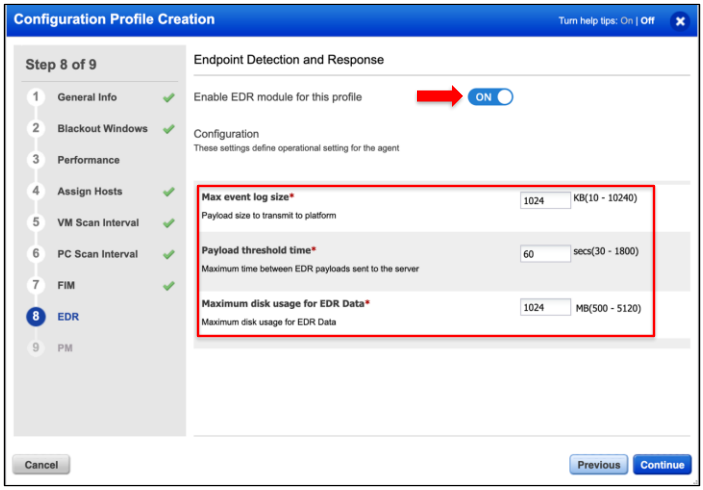
An alternate method is to upgrade existing agent activation keys that are not already enabled for EDR by using the option 'Configure Agents for EDR' from within the EDR app.
This way you can upgrade multiple agent activation keys to use EDR.

On the EDR welcome page, click "Configure Agents for EDR" and select one or more Activation keys to upgrade.

All the agents associated with the activation key/keys will be upgraded and enabled for EDR.

Configuration Profile

- Enable EDR in the Configuration Profile assigned to the target host
- Tune EDR settings (if required)



Agent host assets that require EDR must use a Configuration Profile that is enabled for EDR. This step is performed in the CA app. The EDR module must be turned on in the configuration profile and other EDR settings can be changed from their default values as required.

The following settings apply:

Max event log size

EDR events are transmitted to the Qualys Cloud Platform when the EDR event log file reaches the maximum specified size. You can specify a file size between 10 KB and 10240 KB. Default is 1024 KB. This value can be lower if the Payload threshold time is lower.

Payload threshold time

EDR events are transmitted to the Qualys Cloud Platform when the EDR payload threshold time is hit, i.e., the specified seconds elapse after the previous payload was sent to the Qualys cloud Platform. You can specify a threshold between 30 seconds and 1800 seconds. Default is 60 seconds. This value is lower the better to prevent data loss on busy systems.

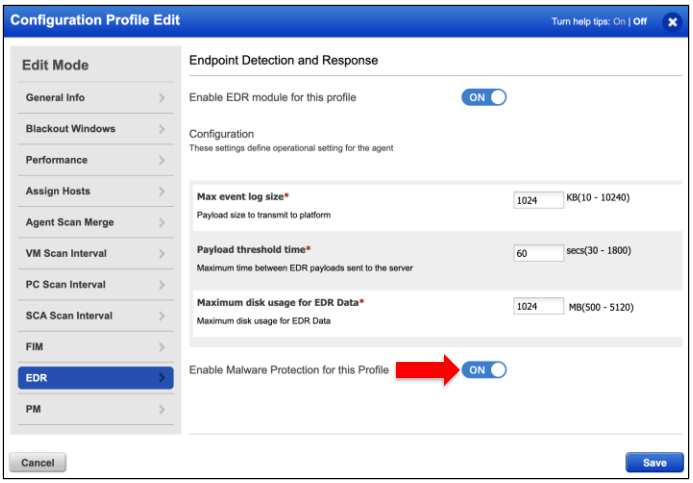
Maximum disk usage for EDR Data

This is the maximum size on disk available to a Cloud Agent for caching EDR events to be sent to the Qualys Cloud Platform for processing. If the maximum size is reached,

the oldest events are deleted in order to create space for newly generated events. You can specify a disk usage size between 100 MB and 2048 MB. Default is 1024 MB.

Malware Protection

- Easily enabled on any endpoint where the Qualys Cloud Agent is installed
- Managed remotely on any endpoint with internet connectivity

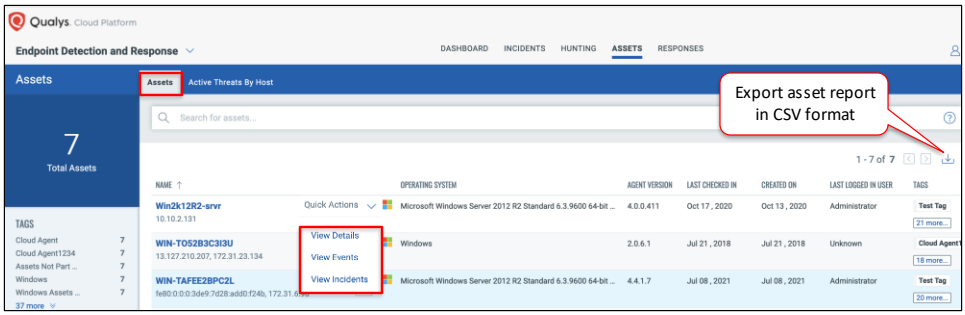


For the agent to start using Malware Protection, this feature must be enabled in the agent configuration profile under EDR.

When the agent host communicates with the Qualys platform, it receives an updated manifest, which is installed with Malware Protection's integrated set of basic virus definitions.
The Malware Protection module starts updating the latest virus definitions as soon as it is installed.

After the latest definitions are downloaded, the AV status is updated in the EDR application under the Assets tab accordingly.

Assets



- Lists all agent hosts activated for EDR
- Contains up to date views on a selected asset's details, its events and incidents
- Asset data can be exported in CSV format

The Assets tab contains a list of agent host assets with the EDR module activated. Here you can get up-to-date views on a selected asset's details, its events, and incidents in one place.

You can also download asset report data in CSV format. When viewing asset details, the user can see asset inventory, vulnerability, compliance, EDR, and other data for the asset in one place.

LAB 1

EDR Activation and Setup



*Please consult **pages 3-7** in the Lab Tutorial Supplement for instructions to perform this lab activity.*

- EDR Activation & Setup, p. 6
- Upgrade Agent Activation Keys, p. 7



Working with the Qualys EDR Application

In this topic, we will provide a quick overview of EDR user interface and the user permissions that are required to manage EDR.

User Interface



- **DASHBOARD** – Contains widgets that monitor important asset, event, incident and malware statistics
- **INCIDENTS** – Contains list of detected incidents across all assets
- **HUNTING** – Contains list of all events and provides remediation actions to fix malicious events
- **ASSETS** – Contains list of agent host assets with EDR module activated and hosts with active infections
- **RESPONSES** – Monitor progress of remediation actions and configure rule-based alerts

30 Qualys, Inc. Corporate Presentation

The EDR user interface is divided into five sections.

DASHBOARDS
Dashboards help you visualize your assets, see your threat exposure, leverage saved searches, and remediate priority of malicious/suspicious events quickly.
We have integrated Unified Dashboard (UD) with EDR. UD brings information from multiple Qualys applications into a single place for visualization.
You can use EDR dashboards provided by Qualys or easily configure your own widgets and dashboards to pull specific information for visualization.

INCIDENTS
This section contains the list of all detected incidents in your environment. Using Qualys advanced search and filter capabilities, you can investigate incidents by Active Threats By Host, Active Threats by Malware name and Malware family name.

HUNTING
This section contains list of all events collected by the Cloud Agent from EDR enabled assets.
Here you can filter and search for events and perform remediation actions for malicious File, Process, Network, and Mutex events.

ASSETS

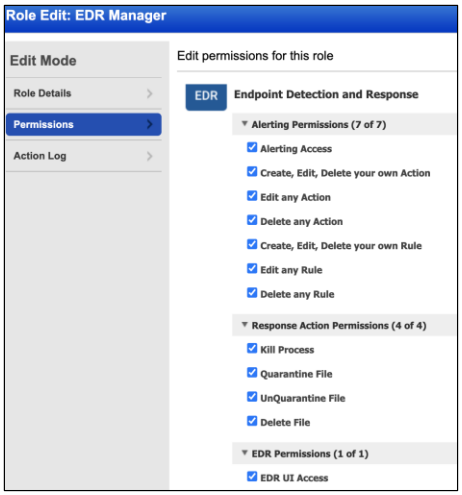
This section contains list of agent host assets with EDR module activated. Here you can get up to date views on a selected asset's details, its events and incidents in one place.

RESPONSES

This section allows you to see request status\progress for remediation actions initiated on malicious events. Here you can also configure EDR to monitor events for conditions specified in a rule and send you alerts if events matching the condition are detected.

EDR Roles and Permissions

- The Manager user for the subscription can assign permissions related to EDR UI/API access, alerting and response actions to non-manager users
- A user with the "EDR Manager" Role has full permissions in EDR
- A Qualys user with the "EDR UI Access" permission can only view the "User Activity" tab under Responses
- EDR Analysts and Incident Responders permissions can be assigned alerting and response action permissions

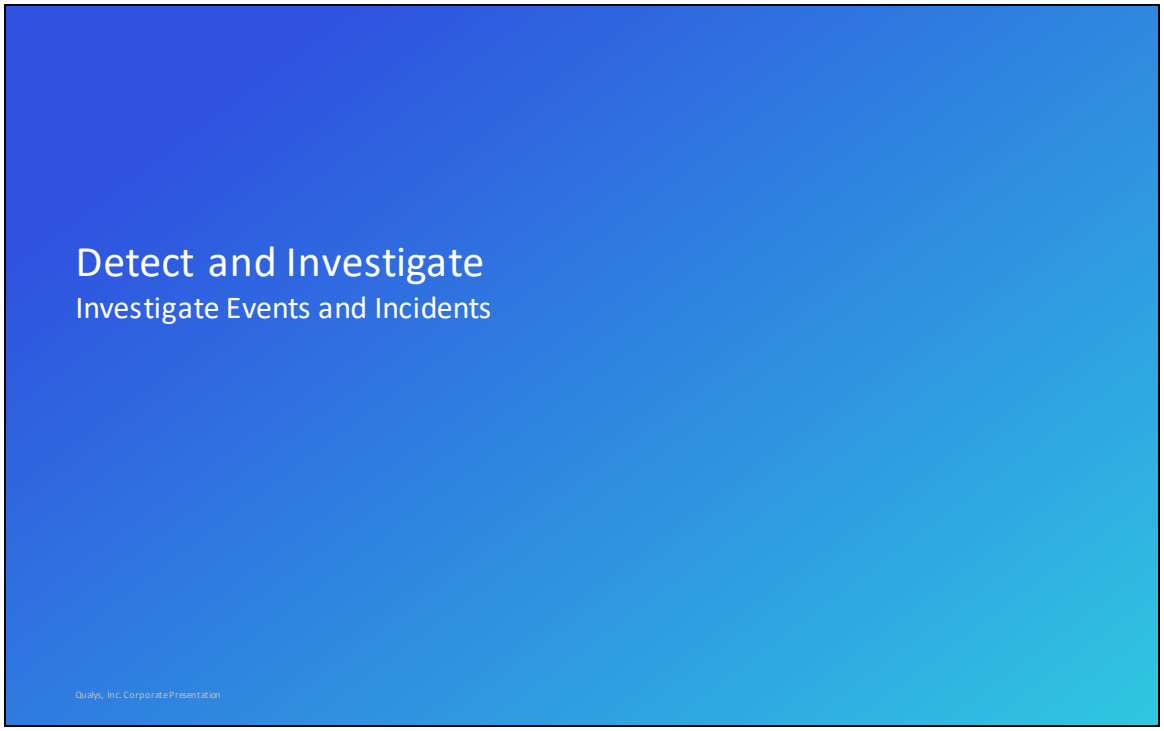


Using the Administration module, the Manager user for the subscription can assign these roles and permissions for all the other users. Depending on the roles and permissions assigned, the user can perform actions like creating, editing, or deleting alert rules and actions.

A user with the Manager role is considered a super-user and has all the available permissions. They have full privileges and access to all modules in the subscription. Only users with Manager role can create other users and assign roles.

EDR User: By default, a Qualys user with the EDR user role assigned has EDR UI permissions only. This user can only see the User Activity tab under Responses.
EDR Analyst, EDR Incident Responder, and EDR Manager: By default, these users have EDR UI and Alerting permissions.

Note: The Manager user can customize the permissions for all the roles.



In this topic, we will understand the various types of events monitored by the EDR agent, the scoring mechanism used to prioritize events and how to identify and investigate assets with malware infections.

EDR Events

- An “object” is an artifact on the system, without state information
- Object Types
  - File – files on locally attached disks (called “image”)
  - Process – a running process, usually from an image
  - Process Network Connection – a network state of a process
  - Mutex – Mutant Handle, a shared memory resource used by processes
  - Registry – Windows, locations used for persistence (auto-start)
- Actions and events include state information:
  - File (Created | Deleted | Renamed | Write)
  - Process (Running | Terminated)
  - Mutex (Running | Terminated)
  - Network (Established | Closed | Listening)
  - Registry (Created | Deleted)

An “object” is an artifact on the system, without state information.

The agent collects data for 5 types of objects:

- File – Portable Executable (PE) and non-PE files (PDF, XLS, PPT, etc.) on local attached disks (called “image”)
  PE is a file format for executables, object code, DLLs and others used in 32-bit and 64-bit versions of Windows operating systems. It is used for EXE,DLL,SYS (device driver) and other file types. Agent collects data for both user files and kernel files. For more information on PE file format, please consult https://docs.microsoft.com/en-us/windows/win32/debug/pe-format

- Process – a running process, usually from an image
- Process Network Connection – a network state of a process
- Mutex – Mutant Handle, a shared memory resource used by processes
- Registry – Windows, locations used for persistence (auto-start)

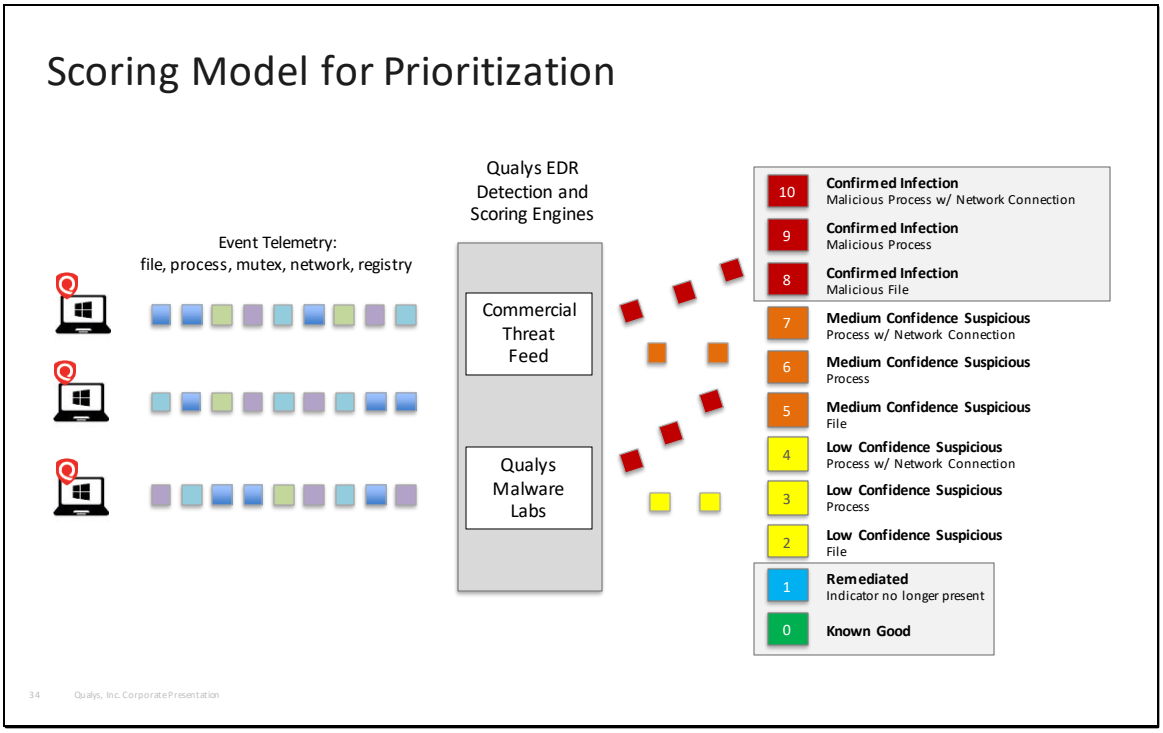
Actions and events on the object include state information. The agent collects data about various objects and associated actions\events on the object in real-time. You can see information about objects along with their state in the EDR app.

An object with its state information:

- File

Created | Deleted | Renamed | Write

- Process
  Running | Terminated
- Mutex
  Running | Terminated
- Network
  Established | Closed | Listening
- Registry
  Created | Deleted



Qualys Threat Scoring model has been developed to ensure you can prioritize threats that have potential for causing more damage. The Threat Score acts as a driver for customer response prioritization (higher response priority for actively running confirmed malware that is communicating, less priority for confirmed file malware that is not persistent and not running)

Confirmed: The events are true malicious code or exhibiting malicious behavior. The detection can be Behavioral or through confirmation from threat intelligence. These events need to be remediated on priority by users.

- Event with **score 10** is confirmed malware, which is performing network activity and needs to be remediated on priority. E.g. Trojan Bot which is connecting to its Command & Control server.
- Event with **score 9** is confirmed malware which is executing and needs to be remediated. Eg. Trojan Horse executing on host.
- Event with **score 8** is confirmed malware file. Eg. Malicious file accidentally downloaded by user or dropped by another malware.

Suspicious – Medium Confidence: These events are highly indicative of malicious code or intent and are mostly Potentially Unwanted Applications (PUA) files.

Suspicious – Low Confidence: Unknown files that have some indication of malicious code or intent but do not have other confirmation or adjudication.

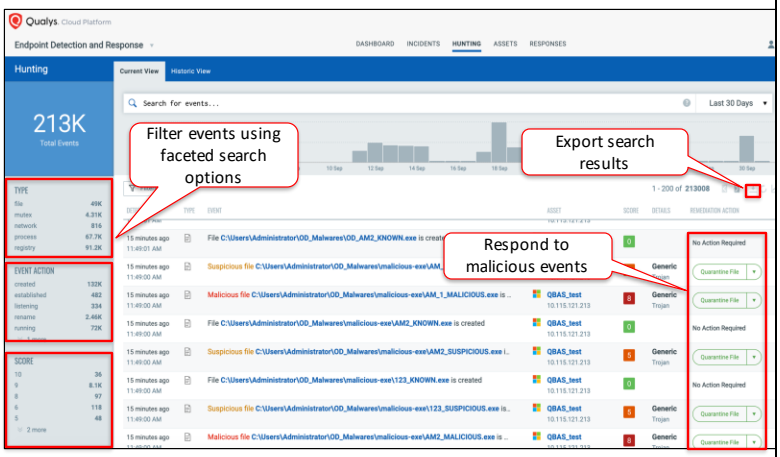
Remediated: The previously scored event is no longer seen on the system due to remediation action performed by user.

Known Good: The event is caused/related to application from known vendor and non-malicious in nature. The source for this can be Qualys whitelist, 3rd party whitelist and Customer whitelist.

Note that registry events are not assigned any score as they do not indicate malicious events on their own.

Hunting

- View event data collected by all EDR agents in one place
- Search for events by event properties, jump to events that occurred in certain time-frame, group events by type, action, and score
- Perform remediation action on malicious file, process, mutex, and network events



The Hunting section contains list of all events collected by the Cloud Agent from EDR enabled assets.
Events are scored on a scale of 0 to 10 using a scoring mechanism for prioritization.

Here you can filter and search for events by event properties, jump to events that occurred in certain time- frame, group events by type, event action and score and view event details and asset details.

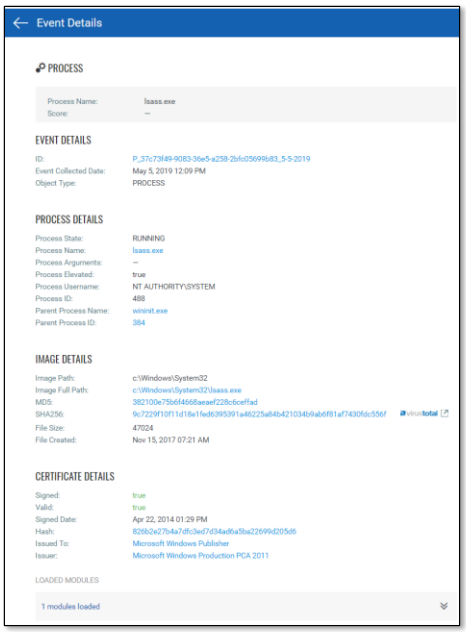
You can also perform remediation actions for malicious File, Process, Network, and Mutex events from this page.

You to download search results to your local system so you can easily manage incidents or events outside of the Qualys platform and share them with other users. You can export results in CSV format.

Event Details

For investigations and analysis

- Event type
- State
- Name
- Elevated
- User
- Process ID
- Parent Process Name / PID
- Image Path
- MD5 / SHA256 hash
- Certificate Details
- Loaded Modules

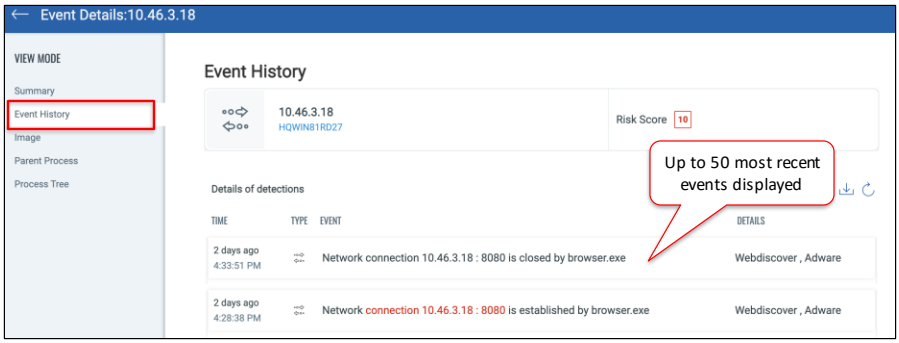


The Events Details page list all the information about the event. To view the Events Details page, click Quick Actions > Event Details.

The Event Details page displays details such as image path, associated user, process ID, MD5/SHA256 hash value, etc. about the object (file/process/mutex/network connection) and the object state (file created, process/mutex running or terminated, network listening on a port, network connection established).

This information aids in threat hunting and is generally required for analysis during a forensic investigation.

Event History



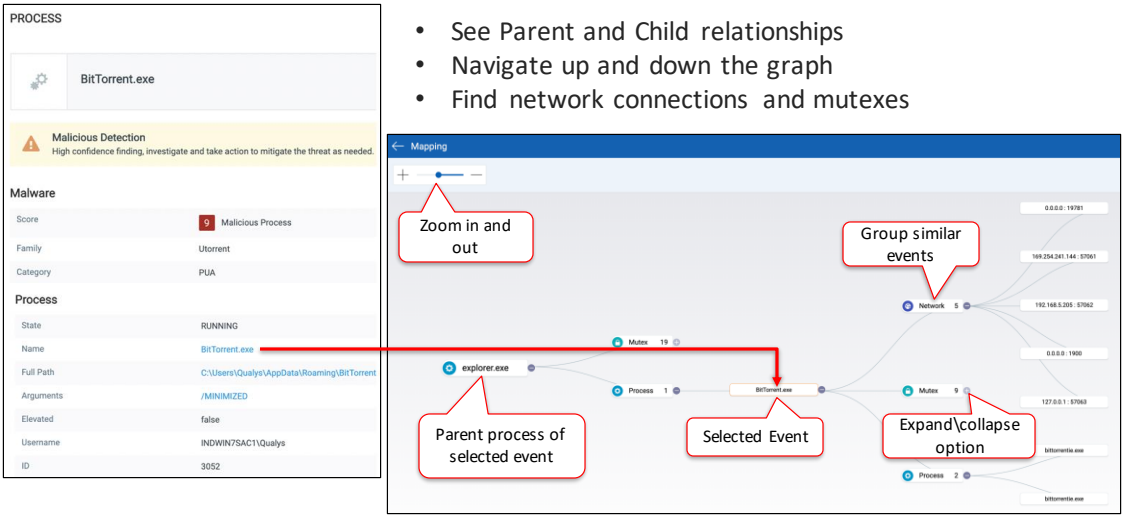
- Agent captures timestamp of every event
- Users can view event lifecycle information (e.g. Process Running then Terminated)
- Can look back to see what happened in the past

The agent captures object (file, registry, process, mutex) and state information in real-time and uploads data to the Qualys cloud platform.

Events are stored as a time series in the EDR Platform and users can view event lifecycle information about current activity as well as events that occurred in the past, in the EDR app.

The Event History tab under Event details shows the detection history of an event. The list shows 50 most recent events for the File, Process, Mutex, Registry, and Network events.

Event Tree- Mapping Related Events



- See Parent and Child relationships
- Navigate up and down the graph
- Find network connections and mutexes

On the Event Details page, we display event tree for Process, Mutex, and Network events.

On the event tree, we display all the events that are related to the selected event.

An event of "Process" type will show its parent and child processes along with the mutex and network connection of the process. For the event of Network type, you see network connection of a process and for the event of Mutex type, mutex connection of a process.

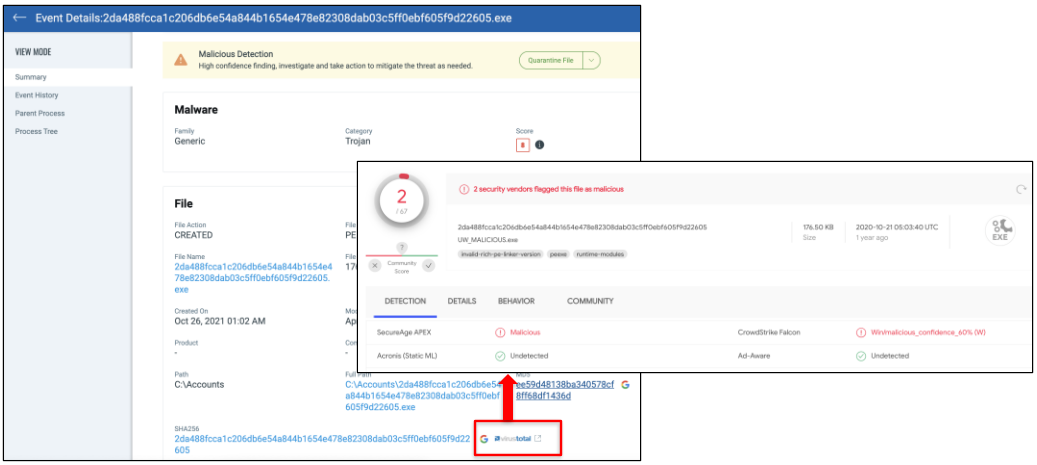
In the event tree view, the selected event node is highlighted with the orange border. You can traverse between the nodes by clicking a node in the hierarchy. You can click on the (+) and (-) to expand and collapse the tree nodes and display the related events.

You can click on the event node to view the details of the selected node. These detail are also displayed on the Event Details Page of that particular event.

To help you identify event types of nodes in a hierarchy view, similar events are grouped under an event type (example: Mutex or Network) and respective event icons are added against the node.

Event's tree view displays a zoom bar to zoom in and out the event's tree. Zoom bar has a plus and minus button for this purpose. It has a re-center button to restore the tree to the center of the screen with its original size.

Verify Findings with Multiple Sources



In this example, a file file is marked malicious with a high confidence score. Here you may want to investigate further.

From the event details page, you can search for the file hash on google to check for available findings/research on this threat or compare EDR findings against the VirusTotal database to cross-verify if other scanning engines have also detected this file/process/mutex as being malicious.

VirusTotal aggregates many antivirus products and online scan engines to check for viruses that the user's own antivirus may have missed, or to verify against any false positives.

In this example, you can see that while some anti-virus engines have flagged this file as malicious.

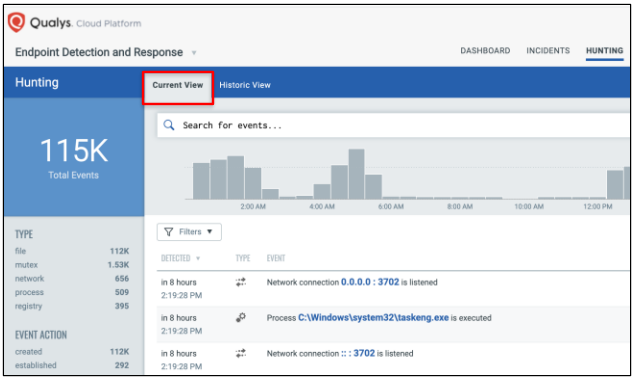
Current View

Active State

"What is happening right now?

Only shows active events from the asset:

- File Created (existence)
- Process Running
- Mutex Running
- Network Listening / Established
- Registry Created (existence)



Current view only shows current activity from the asset pertaining to actions like new file creation, running processes, network connections and so on.

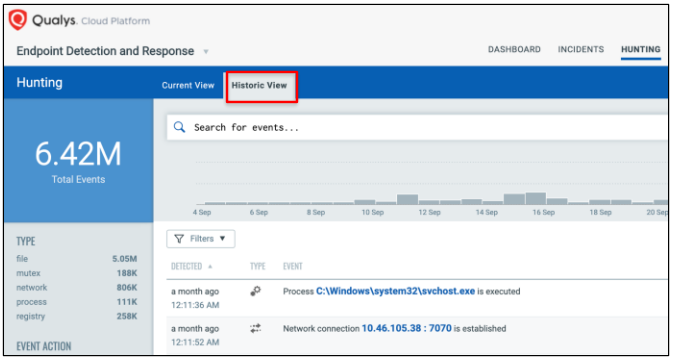
Historic View

"Look Back" Investigation

"What has happened in the past?"

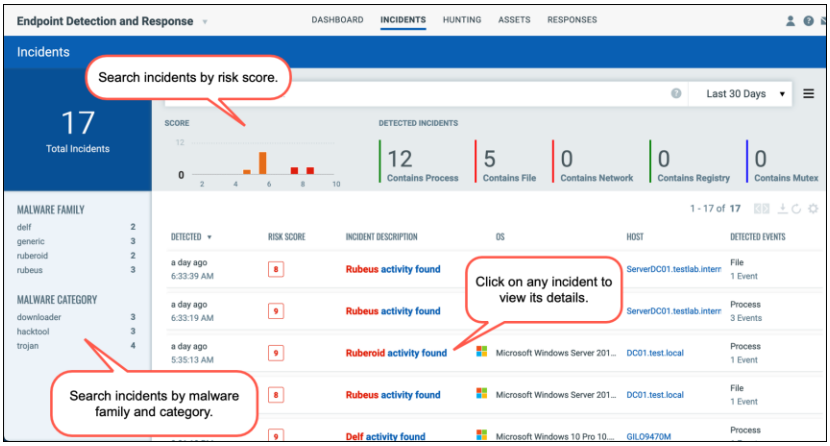
Stored as state change events:

- File Created / Deleted
- Process Running / Terminated
- Mutex Running / Terminated
- Network Listening / Established / Closed
- Registry Created / Deleted



Time series events are stored in EDR Platform for "look back" investigation to see what happened in the past and are displayed under Historic View.

Incidents



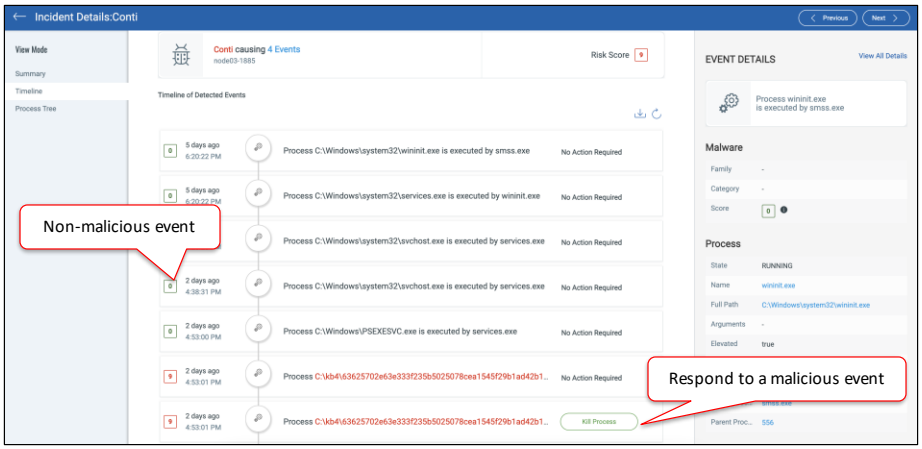
- An incident is comprised of one or more events associated with a malware infection
- Risk Score of a host incident is based on the highest single event score

The Incidents section displays the list of all detected incidents in your environment across all EDR assets.

Here too, you can filter threats by Malware Family names and by Malware categories.

You can drill-down into an incident to see event details. This will automatically redirect the search to the Hunting section from where you can take remediation action on prioritized events.

Incident Timeline

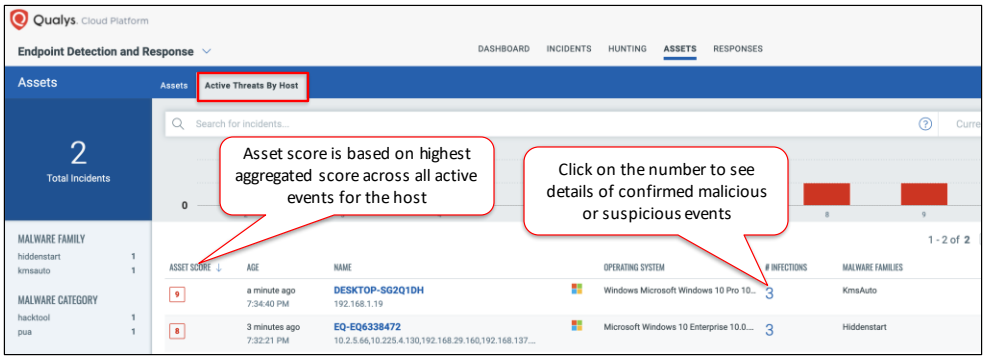


In the Incidents Details, view information like Timeline, Process Tree, Asset Details, etc.

Navigate to the Timeline tab to view the timeline of the detected event and choose a remediation action if applicable.

If the risk score is zero, then the incident is considered remediated or non malicious.

Active Threats by Host



- Investigate confirmed or suspected infections on identified hosts
- Combine Asset score with the host vulnerability and patch status to prioritize remediation along with patching

The Active Threats by Host tab displays all hosts with confirmed or suspected infections.

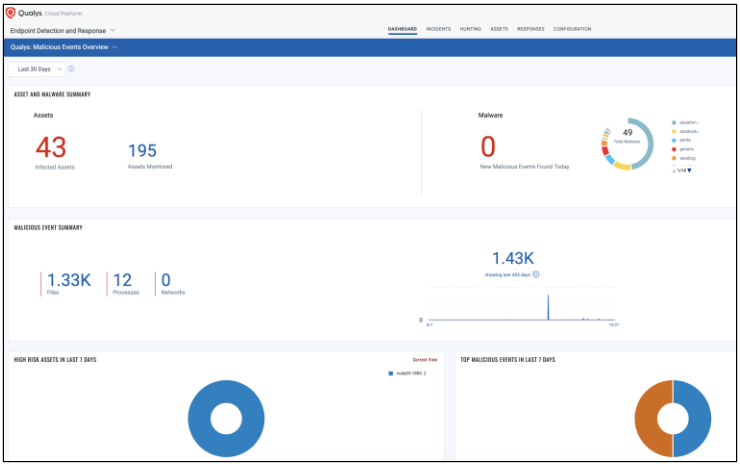
You can filter hosts with infections by Malware Family names such as zbot, Keybase, Backoff, GlassRAT,etc. and by Malware categories such as backdoor, PUA, rootkit, trojan, etc.

Asset Score
This is a model to score an asset. The highest event score is the asset's score during the selected time period.
The asset's score can dynamically change as new events come in, eg. known bad file (asset score 8), process launches from that file (asset score 9), process terminates leaving only bad file (asset score 8), etc.

The asset score combined with the host vulnerability and patch status helps to prioritize remediation along with patching.

Dashboards

- Looking at individual assets or events and incidents for investigation can be time consuming
- Visualize your assets and threat exposure, leverage saved searches, and remediate malicious events quickly
- Use Unified Dashboards to pull information from multiple Qualys applications in one place



Dashboards are interactive reports and offer a powerful way to visualize data in one place
You can use EDR dashboards provided by Qualys or easily configure your own widgets and dashboards to pull specific information for visualization.

Dashboards help you visualize your assets, see your threat exposure, leverage saved searches, and remediate prioritized malicious/suspicious events quickly.

We have also integrated Qualys Unified Dashboard (UD) with EDR. This brings information from multiple Qualys applications into a single place for visualization so that you have all the information you need in one place thereby providing a better context for remediation.

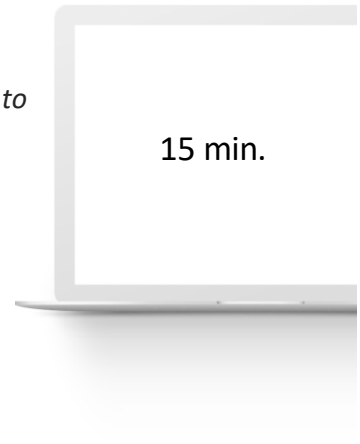
LAB 2

EDR Events & Incidents

PLAY

*Please consult **pages 8-12** in the Lab Tutorial Supplement for instructions to perform this lab activity.*

- EDR Events, p. 11
- EDR Incidents, p. 12



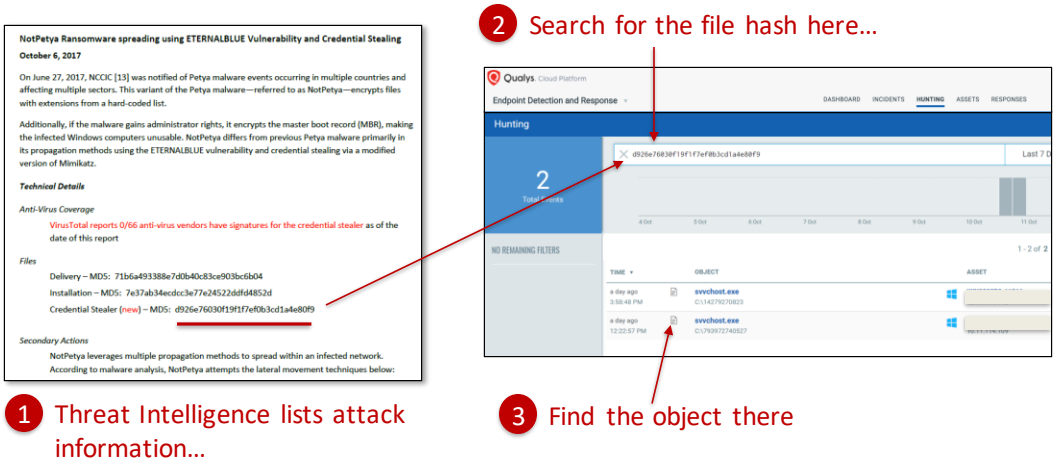
Detect and Investigate

Hunt for Threats

Qualys, Inc. Corporate Presentation

In this topic, we will discuss how to verify threat intel and perform threat hunting using threat hunting queries.

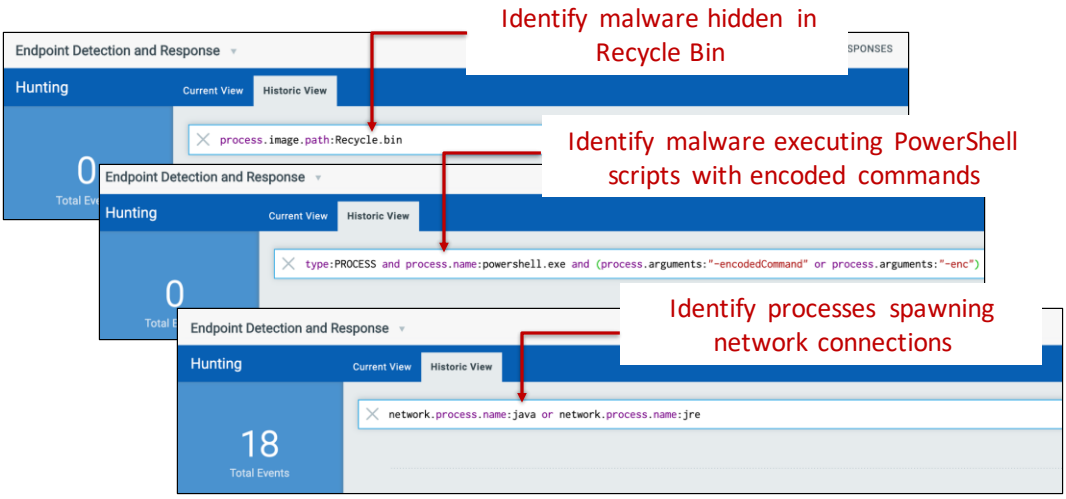
Threat Intel Verification


NotPetya Ransomware spreading using ETERNALBLUE Vulnerability and Credential Stealing
October 6, 2017
On June 27, 2017, NCCIC [13] was notified of Petya malware events occurring in multiple countries and affecting multiple sectors. This variant of the Petya malware—referred to as NotPetya—encrypts files with extensions from a hard-coded list.
Additionally, if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable. NotPetya differs from previous Petya malware primarily in its propagation methods using the ETERNALBLUE vulnerability and credential stealing via a modified version of Mimikatz.
Technical Details
Anti-Virus Coverage
VirusTotal reports 0/66 anti-virus vendors have signatures for the credential stealer as of the date of this report
Files
Delivery – MD5: 71b6a493388e7d0b40c83ce903bc6b04
Installation – MD5: 7e37ab34ecdcc3e77e24522ddfd4852d
Credential Stealer (new) – MD5: d926e76030f19f1f7ef0b3cd1a4e80f9
Secondary Actions
NotPetya leverages multiple propagation methods to spread within an infected network. According to malware analysis, NotPetya attempts the lateral movement techniques below:
2 Search for the file hash here...
Qualys. Cloud Platform
Endpoint Detection and Response
DASHBOARD
INCIDENTS
HUNTING
ASSETS
RESPONSES
Hunting
d926e76030f19f1f7ef0b3cd1a4e80f9
Last 7 D
2
NO REMAINING FILTERS
1 - 2 of 2
TIME
OBJECT
ASSET
svchost.exe
svchost.exe
1 Threat Intelligence lists attack information...
3 Find the object there

A commonly-shared form of threat intelligence as practiced today is the sharing of host-based indicators for malicious code, which are most often file names and hashes. This example describes a file hash indicator and the name and type of the piece of malware that it indicates. Searching for the hash in this scenario might indicate if a sample of NoPetya ransomware is present in your environment.

You can simply search for the hash value in the Hunting section and EDR will identify any objects matching the given hash. From there, you can take an appropriate response action to contain the malicious event.

Hunting for Threats



49 Qualys, Inc. Corporate Presentation

This slide illustrates a few examples of using search queries to look for suspicious activity.

What file properties are interesting?

- Examine signer/certificate information
- Look for files running out of $RECYCLE.BIN, %temp% or %downloads%

How do you look for evasion techniques?

- Malware files may be named to pose as native Windows files
- Compare filenames within %system% to files on disk
- Look for suspicious use of SVCHOST, WMI, PowerShell

Are your files trusted?

- Examine certificate information
- Enrich findings by looking for persistent untrusted files, untrusted processes, untrusted processes generating network traffic

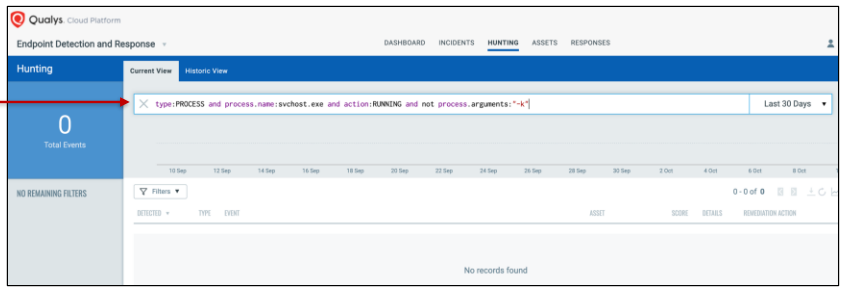
Sample Hunting Search

Threat Actor Tactic and Hunting Approach – "Suspicious Use of SVCHOST":

- Service Host ("svchost.exe") is a system process that hosts multiple Windows services.
- Normal usage is to use the "-k" argument to define the service (via DLL) to instantiate, e.g. "svchost.exe -k imgsvc". This will display the service name that is loaded by svchost.
- Threat actors try to evade detection by injecting malware directly into svchost.exe, thus there is no "-k" argument.
- Hunting approach: svchost.exe running without "-k" argument is suspicious.

EDR search logic: Find all running svchost.exe processes that do not have "-k" as an argument.

(this will find all current and past instances, even if the machine is offline or rebuilt)



50

Scenario

Service Host ("svchost.exe") is a system process that hosts multiple Windows services.

Normal usage is to use the "-k" argument to define the service (via DLL) to instantiate, e.g. "svchost.exe -k imgsvc". This will display the service name that is loaded by svchost. Threat actors try to evade detection by injecting malware directly into svchost.exe instead of calling their code directly, thus there is no "-k" argument.

Goal

Find all running svchost.exe processes that do not have "-k" as an argument.

EDR Search Query

```
type: PROCESS and process.name: svchost.exe and
action:RUNNING and not process.arguments: "-k"
```

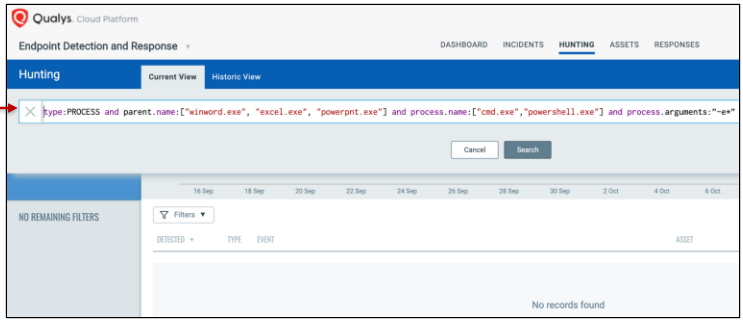
Sample Hunting Search

Threat Actor Tactic and Hunting Approach – "Suspicious Use of Windows Command Shell and PowerShell":

- Threat actors try to evade detection by running malicious scripts directly into memory using whitelisted programs
- Normal usage does not involve PowerShell or cmd.exe invocation through MS Office programs
- Hunting approach: winword.exe or excel.exe or powerpnt.exe running launching cmd.exe or powershell.exe

EDR search logic: Find all running MS Office processes that have invoked the windows command shell or PowerShell

(this will find all current and past instances, even if the machine is offline or rebuilt)



Threats such as fileless attacks involve use of legitimate\whitelisted programs such as Windows command shell\PowerShell to load malware directly into memory.

Although Microsoft's PowerShell is preinstalled on nearly all Microsoft systems and is considered trusted software, seeing it launched via MS word or powerpoint or Excel is highly anomalous and suspicious.

The following search query will identify any MS office processes such as winword.exe, excel.exe, powerpoint.exe and others invoking Windows command shells:

```
type:PROCESS and parent.name:["winword.exe", "excel.exe",
"powerpnt.exe"] and
process.name:["cmd.exe","powershell.exe"] and
process.arguments:"-e*"
```

Looking further into the process tree may reveal if these trusted applications are being used to execute any suspicious files that PowerShell wrote. The attacker could even use encoded commands in Base64 to further obfuscate the malicious activity to evade legacy antivirus and other traditional means of detection. Although each of these binaries might be trusted or signed, executing with encoded commands could be an indicator of a malicious attack.

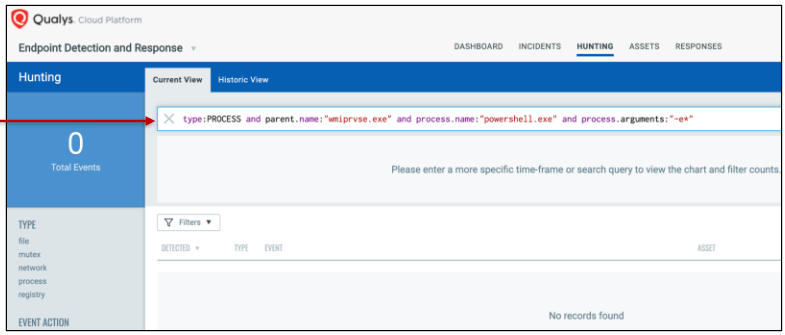
Sample Hunting Search

Threat Actor Tactic and Hunting Approach – "Suspicious Use of WMI":

- WMI ("wmiprvse.exe") is a system process that runs WMI commands on a remote host
- Threat actors use it as a remote execution utility and to establish persistence
- Hunting approach: powershell.exe running with wmiprvse.exe as parent process may be suspicious

EDR search logic: Find all running PowerShell processes that are WMI-invoked

(this will find all current and past instances, even if the machine is offline or rebuilt)



WMI was developed as Microsoft's interpretation of web-based enterprise management (WBEM) for system management and auditing; however, adversaries can use it for all stages of the Attack Lifecycle, from creating the initial foothold on a system to stealing data from the environment and everything in-between (common use is a as a remote execution utility and persistence mechanism to execute malware).

WMI is incredibly flexible, and attackers have identified many ways to run malicious code using it.

Finding malicious WMI and PowerShell in memory can be challenging due to the amount of legitimate activity happening in the modern enterprise. As with all things hunting, context is important, and we can often get more context by looking at the parent and children of processes.

WmiPrvSE.exe process (WMI Provider Host) is responsible for running WMI commands on a remote (target) system. WmiPrvSE facilitates the interface between WMI and operating system. The children of a WmiPrvSE process can often be the clue that helps identify suspicious behavior.

The following query will search for instances of PowerShell spawning via WMI:
`type:` `process` ` and parent.name:"wmiprvse.exe"`

```
and process.name:”powershell.exe”
and process.arguments:”-e*”
(the argument –e* will look for encoded powershell
commands which indicates suspicious activity)
```

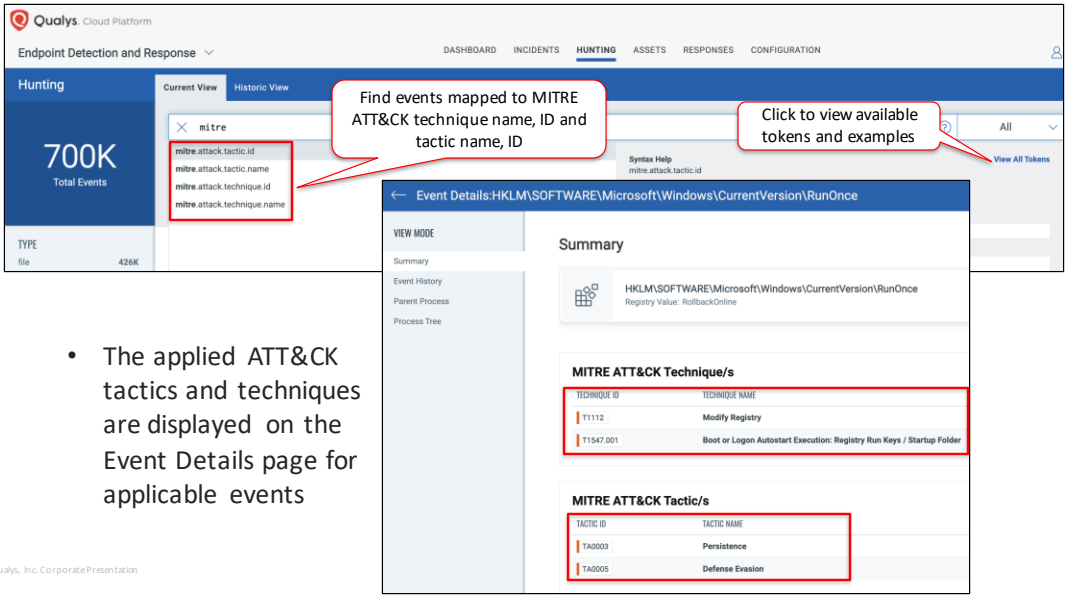
Leverage MITRE ATT&CK Framework

- MITRE ATT&CK defines the tactics, techniques, and procedures that are leveraged by adversaries and malware
- EDR helps detect malicious behavior on the endpoint by evaluating the events in context with MITRE ATT&CK
- Having ATT&CK context aids analysts when hunting for and responding to incidents

MITRE ATT&CK defines the tactics, techniques, and procedures that are leveraged by adversaries and malware. MITRE ATT&CK is more behavioral focused that analyzes when humans or malware leverage the built-in operating system binaries, utilities, or capabilities which otherwise might not be malicious on their own.

EDR helps detect malicious behavior on the endpoint by evaluating the events in context with MITRE ATT&CK. Having ATT&CK context also aids analysts when hunting for and responding to incidents within their environment.
With each release, Qualys will continue to add more rules to help classify the events appropriately.

Filter Events Mapped to MITRE ATT&CK

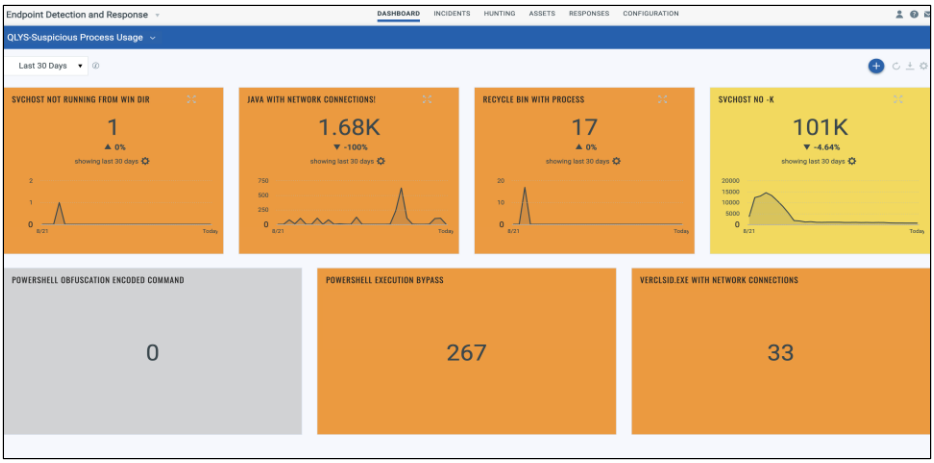


- The applied ATT&CK tactics and techniques are displayed on the Event Details page for applicable events

You can find events with the MITRE ATT&CK framework technique name or ID and the tactic name and ID in the Hunting tab.

We have added the following four MITRE ATT&CK tokens on the Hunting tab:
mitre.attack.tactic.id: This token will help you find events with the tactic ID from the MITRE ATT&CK framework.
mitre.attack.tactic.name: This token will help you find events with the tactic name from the MITRE ATT&CK framework.
mitre.attack.technique.id: This token will help you find events with the technique ID from the MITRE ATT&CK framework.
mitre.attack.technique.name: This token will help you find events with the technique name from the MITRE ATT&CK framework.

Dynamically Track the Attack Surface



Leverage dashboards to automatically get a dynamically updated picture of the entire threat landscape

You can use the threat hunting queries illustrated earlier to build dashboard widgets to get up to date information on malicious and suspicious events, remediation actions, assets with malware associations, etc. in one place.

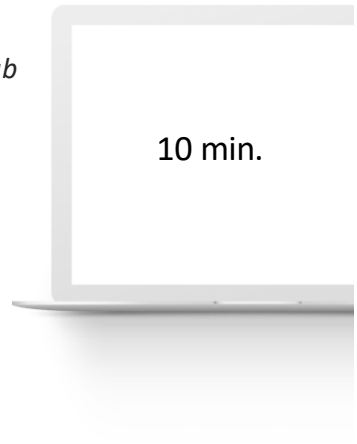
Clicking on any of the widget will redirect the search to the Hunting section. Here, you can then view event details for specific events to understand more about the threat.

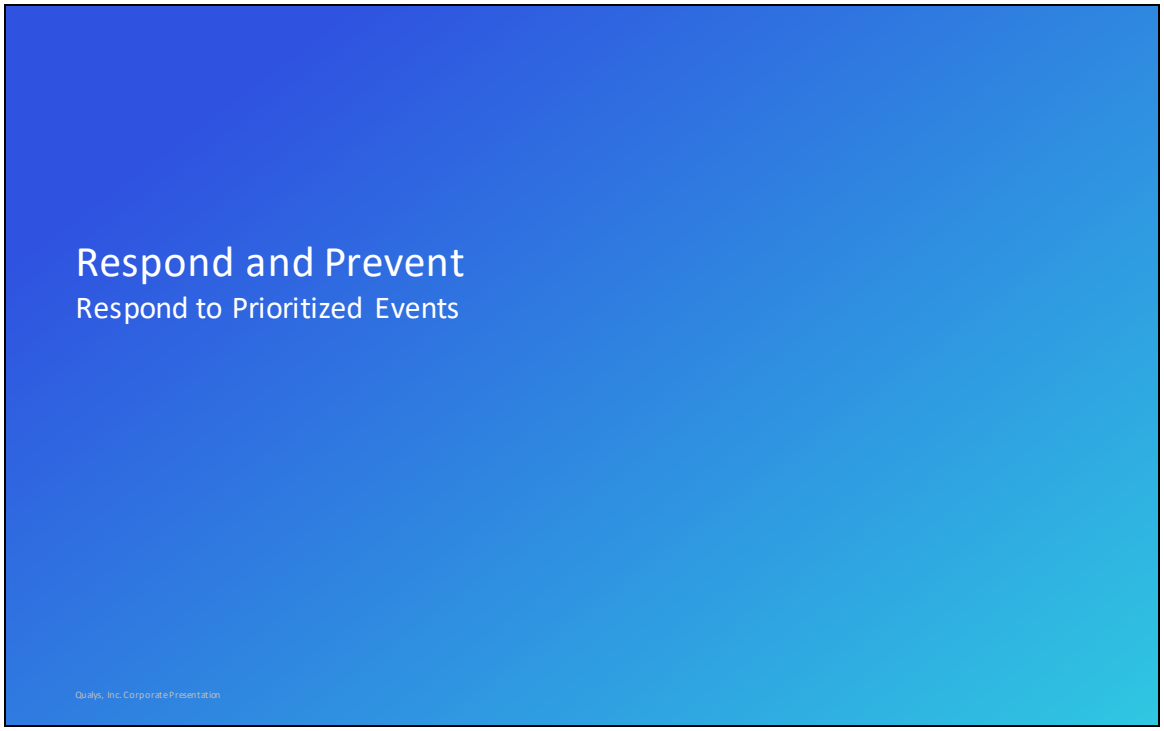
LAB 3

Hunt for Suspicious Activity

PLAY

*Please consult **pages 13-17** in the Lab Tutorial Supplement for instructions to perform this lab activity.*





In this topic, we will discuss the available response actions in EDR to remediate malicious events.

Response Actions

Remediation actions for malicious **file** events:

- **Quarantine File**
  - File is encrypted and then moved to the Quarantine folder on asset
  - Quarantine folder automatically created once you upgrade to agent 4.0 and above
  - Can undo this action and restore the file to its original position using the **UnQuarantine** file option
- **Delete File**
  - File is permanently deleted from your asset
  - Cannot undo this action

Remediation actions for malicious **process, mutex,** and **network** events:

Kill Process

- Kills the malicious process and its corresponding parent process, if any

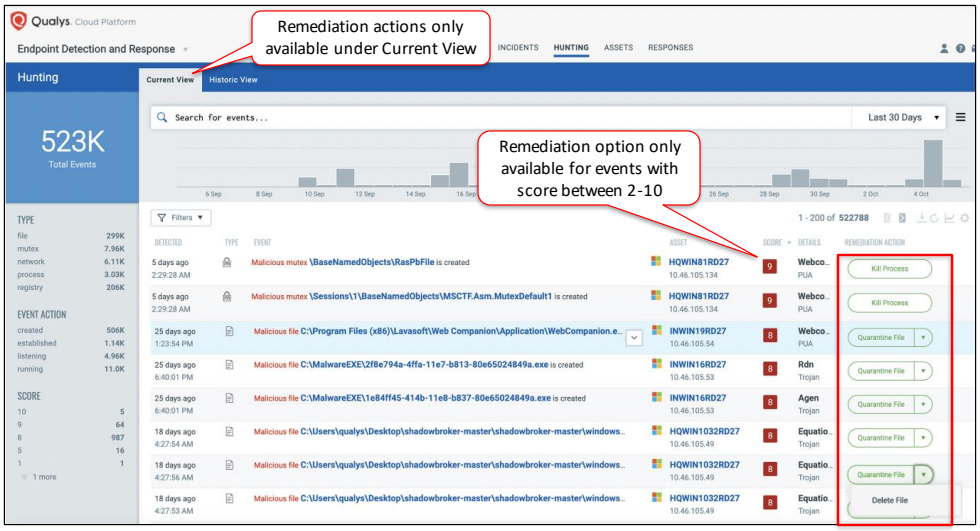
58 Qualys, Inc. Corporate Presentation

You can remediate malicious file events, using the following options:

- **Quarantine File**: Using this option, the file is encrypted and then moved to the Quarantine folder (C:\ProgramData\Qualys\QualysAgent\Quarantine\) on your asset. The Quarantine folder is automatically created once you upgrade to Cloud Agent 4.0 and above. You can undo this action and restore the file to its original position using the UnQuarantine option from the User Activity tab. For more information, see UnQuarantine File.
- **Delete File**: Using this option, the file is permanently deleted from your asset. You cannot undo this action.

For process, mutex, and network events, we provide **Kill Process** remediation action. When you perform the Kill Process action for mutex or network events, it kills the corresponding parent process.

Response Actions



Remediation actions can be performed for File, Process, Network, and Mutex events from the Hunting section and from the Event Details page.

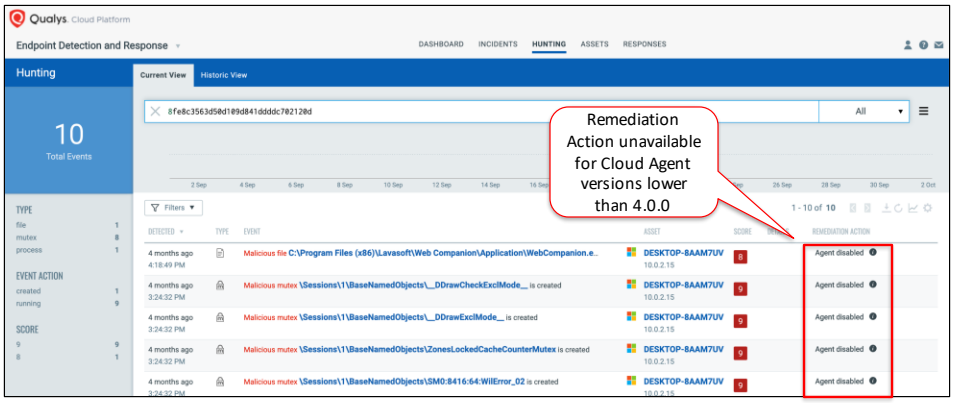
The remediation options are available under the Remediation Action column and Events Detail page only for:
- Events in Active\Current View
- Events that score between 2 to 10

You can remediate malicious events on assets using the Quarantine File, Delete File, and Kill Process options.

The UnQuarantine action is only available for files that were previously quarantined. This action will decrypt the quarantined file in the Quarantine folder (C:\ProgramData\Qualys\QualysAgent\Quarantine\) and move it back to the original location.

You can also retry the remediation action on failed events from this page.

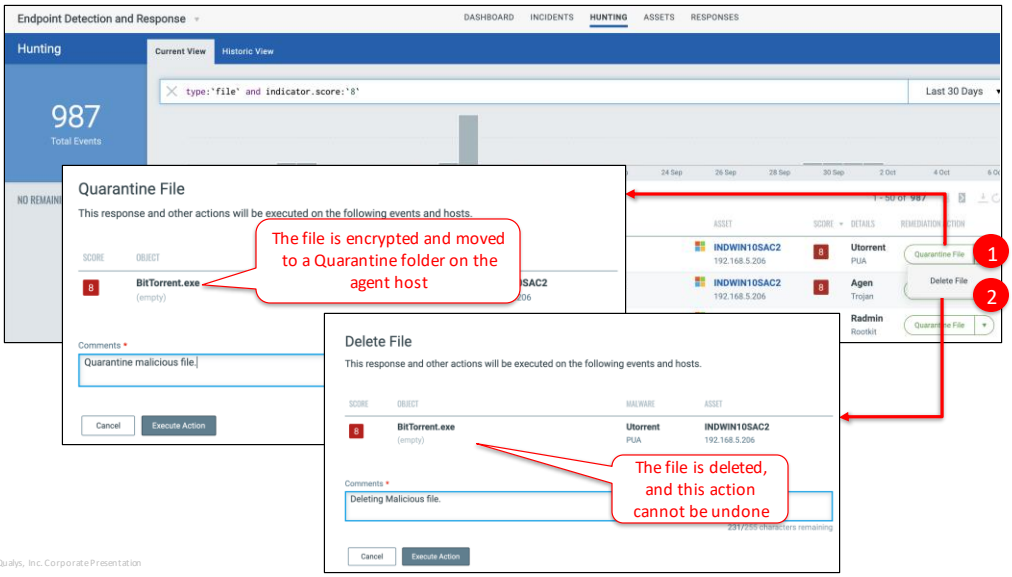
Response Action for Older Agents



Full EDR functionality is only available for Cloud Agent versions 4.1 and above for Windows.

Note that response actions are only available for Cloud Agent version 4.0.0 and above for windows assets. While event data is still collected and processed for older EDR agents, remediation actions are not available for such agents.

Response Actions for File Events



Perform the following actions to respond to a file type of event:

1. Select the required file event and from the Remediation Action column, click Quarantine File or Delete File from the drop-down list.
   Note: You can also perform the remediation action from the Event Details page.

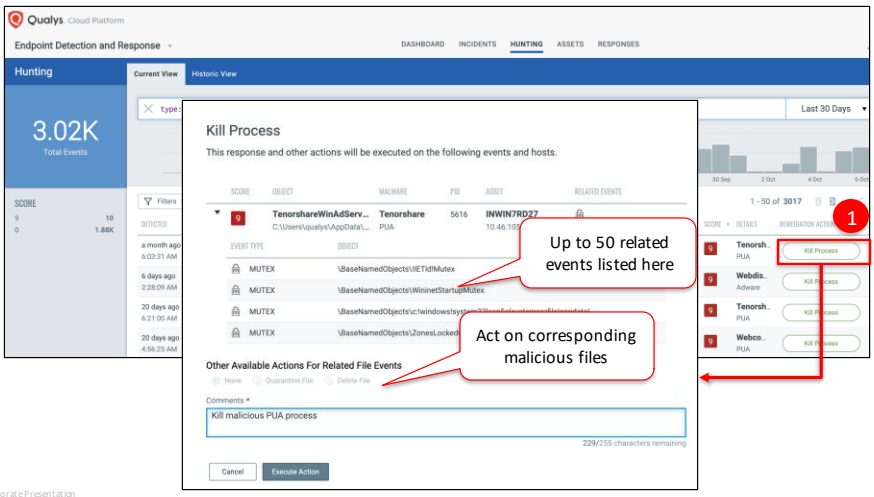
2. Based on your selection (Quarantine File/Delete File), one of the window as displayed in the illustration is displayed.

3. Enter a comment describing the reason for this action (this is not optional)

4. Click Execute Action to complete the response action.

A pop-up message indicating the status of submission request is displayed on the screen. You can click View Request Status from the pop-up message, to view the status (In Progress, Success, Failed) of the remediation request on the User Activity tab under the Responses section. Alternatively, you can also view the status for the remediation request from the Remediation Action column on the Hunting tab.

Response Action for Process, Mutex and Network Events



Perform the following actions to respond to a process, mutex or a network type of event:

1. Select the required event from the Hunting tab and from the Remediation Action column, select Kill Process.
   Note: You can also perform the remediation action from the Event Details page.
   The Kill Process screen is displayed. Under Related Events column, you can see the related file, network, and mutex events.

2. Use the arrow button next to the Score column to view the list of related events.
   Note: We display up to 50 related events.
   If the event has related files, you can choose to Quarantine file, Delete files or perform no action by selecting None.

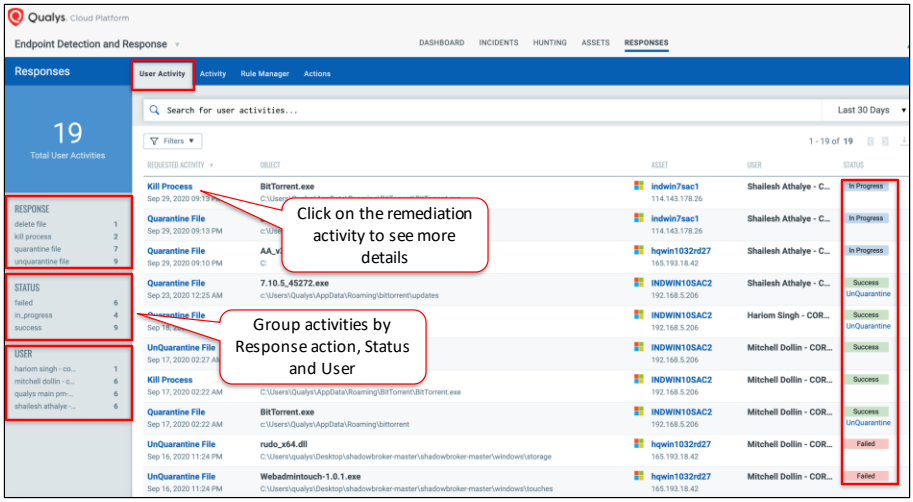
3. Enter a comment describing the reason for this action (this is not optional)

4. Click Execute Action to complete the response action.

A pop-up message indicating the status of submission request is displayed on the screen. You can click View Request Status from the pop-up message, to view the status (In Progress, Success, Failed) of the remediation request on the User Activity tab under the Responses section. Alternately, you can also view the status for the

remediation request from the Remediation Action column on the Hunting tab.

Monitor Remediation Activity

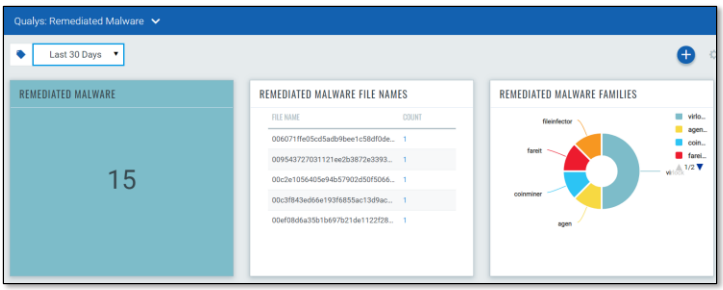


The User Activity page under the Responses section lists all the remediation activities performed on events, with the following details:

- The requested remediation action along with the date and time
- The object (file/process) and the asset on which the action is performed
- The user who performed the remediation action
- The current status of the remediation action

Here you can group activities by the Response action type (delete\quarantine\unquarantine file, kill process), by activity Status (success, failed, in progress) and by the Qualys User who performed the action.

Track Remediations and Reoccurrence



- Dynamically track infections trend vs remediation
- Ensure malware has been eradicated from devices
- Tracks reoccurrence over time to find if a host is getting re-infected

The EDR agent continues to monitor assets for malicious activities and identifies if a malware that was previously detected is no longer present on an asset.

You can use dashboard widgets to track remediations and to find if a host is getting re-infected over time.

It is important to identify and eliminate the root cause of a malicious event in order to prevent its reoccurrence. Many a times, malware finds its way in an environment if issues such as exploitable vulnerabilities, misconfigurations, obsolete software, missing patches, etc. are left unaddressed. So, in addition to taking remediation actions in EDR, you also need to eliminate the root cause to prevent a malware from resurfacing in the environment. EDR together with VMDR and Patch Management (PM) helps you achieve this goal.

LAB 4

Perform Remediation Action

PLAY

*Please consult **page 18** in the Lab Tutorial Supplement for instructions to perform this lab activity.*



Respond and Prevent

Configure Rule-based Alerts

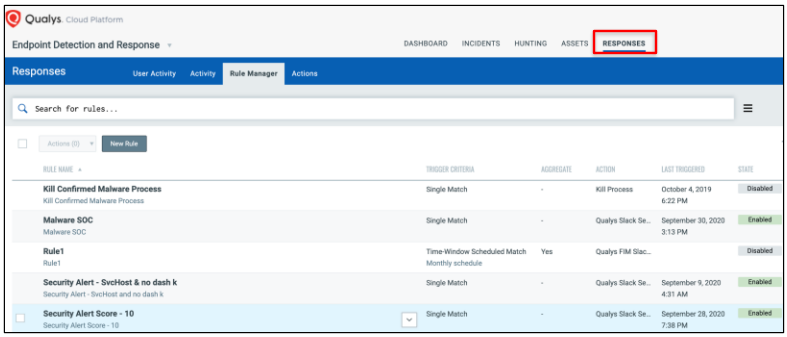
Qualys, Inc. Corporate Presentation

In this section, we will provide an overview of configuring rule-based alerts to notify users through various channels when malicious events are detected in the environment.

Alerting

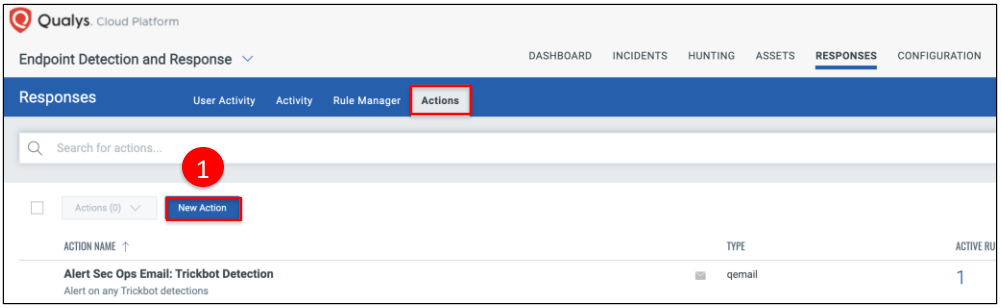
Immediately notify your teams of important events impacting the overall health and security hygiene of critical assets.

- Rule/QQL driven alerts
- Out-of-box templates /examples
- Notification via Email, Slack & PagerDuty



In order to effectively manage your threat landscape, you should setup Responses (notifications) to alert you about conditions requiring attention (e.g. confirmed malicious process with a network connection, Mitre ATTA&CK technique-based detection for privilege escalation, etc.).
You can configure rules to monitor critical events that satisfy the conditions specified in a rule and send you alert messages if events/incidents matching the condition are detected. The alert message will have the event details.

Configure New Action

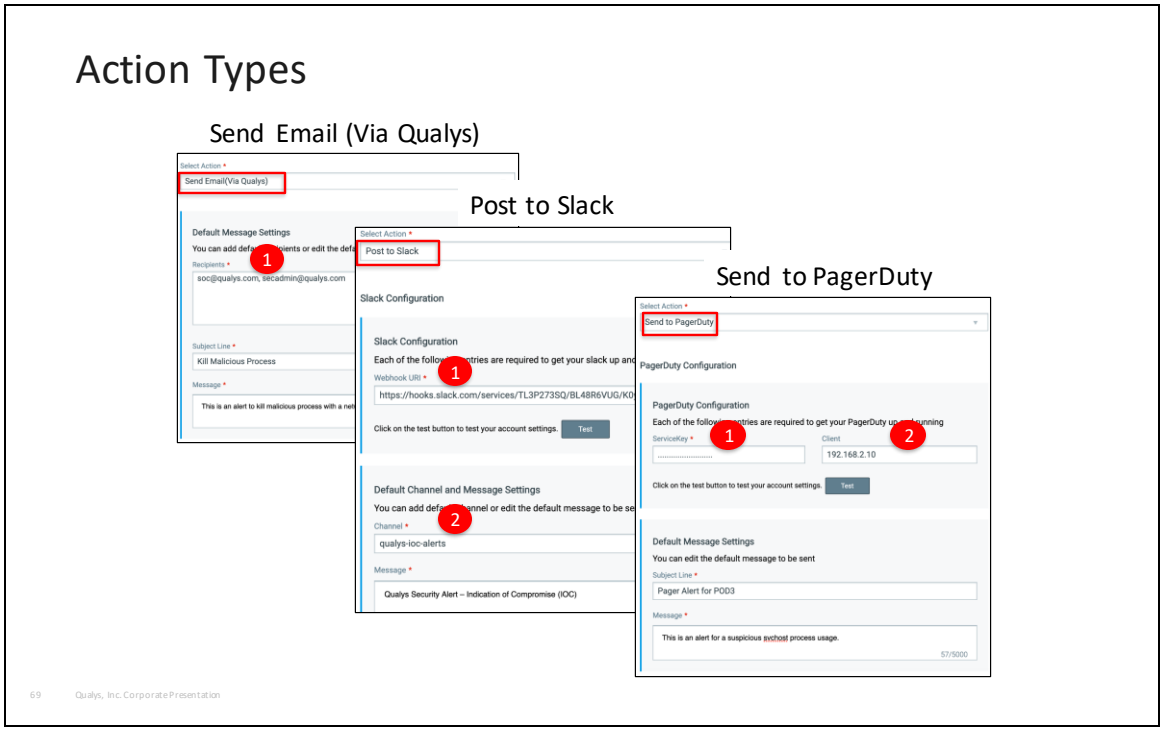


Step 1: Configure a rule action that will be referenced in the alert rule.

The first step is to configure a rule action that will be referenced in the alert rule. You can configure a rule action under the Actions tab in the Response section.

Provide a name and a description for the action and select an action from the Select Action drop-down.

Provide the settings for configuring the messaging system that Qualys will use to send alerts.



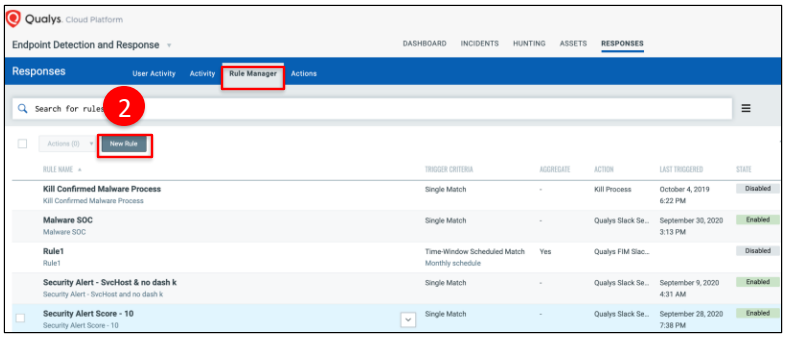
EDR supports these three actions:

1. Send Email (Via Qualys)
Select Send Email (Via Qualys) to receive email alerts and specify the recipients' email ID who will receive the alerts, subject of the alert message and the customized alert message.

2. Post to Slack
Select Post to Slack to send alerts to your Slack channel. Provide the webhook URL and the Slack channel you want to post the alerts to. In Default Message Settings, customize the alert message, if necessary.

3. Send to Pager Duty
Select "Send to PagerDuty" to send alerts to your PagerDuty account. Provide the API service key and the client that EDR will require to connect to your PagerDuty account. In Default Message Settings, specify the subject and the customized alert message.

Configure New Rule



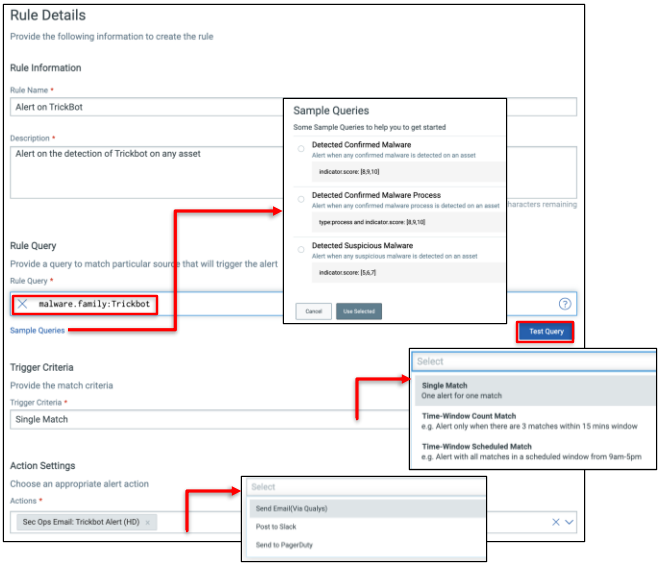
Step 2: Configure a rule specifying events you want to monitor, criteria for triggering the rule and actions to be taken on those events.

The next step is to configure a rule to generate alerts for critical events. You can configure rules under the Rule Manager tab in the Response section.

When a rule is triggered based on a condition match, EDR will send you alerts using the configured action type that will have details of the events.

Rule Settings

- Define a search query to filter events for alerting
- Use the "Test Query" button to look for any current event matching the set criteria
- Select criteria to define when notifications are triggered
- Select an action from the configured action types



The next step is to configure a rule to generate alerts for malicious events. You can configure rules under the Rule Manager tab in the Response section. Provide required details in the respective sections to create a new rule.

Click **Sample Queries link** to select from predefined queries.

You can choose from three trigger criteria that work in conjunction with the rule query. The **Trigger criteria** are: Single Match, Time-Window Count Match and Time-Window Scheduled Match.

In the **Action Settings** section choose the actions that you want the system to perform when an alert is triggered.

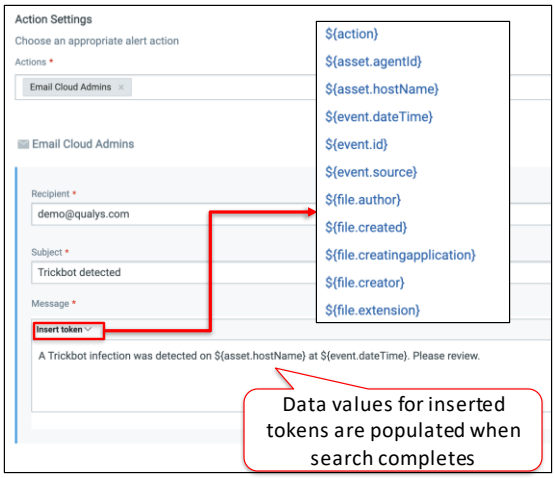
Trigger Criteria

- Select Single Match if you want the system to generate an alert each time the system detects an event matching your search query.
- Select Time-Window Count Match when you want to generate alerts based on the number of events returned by the search query in a fixed time interval. For example, an alert will be sent when three matching events are found within 15 mins window.
- Select Time-Window Scheduled Match when you want to generate alerts for matching events that occurred during a scheduled time. The rule will be triggered

only when an event matching your search criteria is found during the time specified in the schedule. Choose a date and time range for creating a schedule and specify how often you want to run the schedule for example, daily, weekly and monthly. For example, send daily alerts with all matches in a scheduled window between 4 pm and 5 pm. For the Weekly option, select the days of the week on which schedule will run. For example, send weekly alerts with all matches generated between 4.56 pm and 5.56 pm on every Monday and Wednesday. For the Monthly option, specify the day of the month on which the schedule will run. For example, send monthly alerts on the first day of every month.

Insert Tokens

- Insert tokens in the message body to include relevant asset and event information within the alert message
- Supported for all action types (Email, Slack, PagerDuty)
- Only tokens that help in asset and event scoping or those that are directly related to the alert evaluation are supported



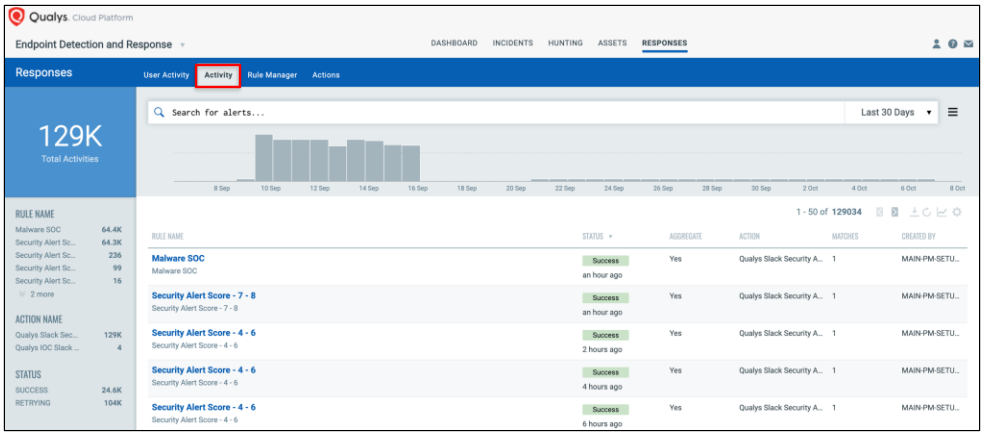
The Recipient, Subject and Message are automatically populated within the rule based on the selected Actions type.

Qualys also supports use of tokens within the message body which work as placeholders or variables for data values that populate when the search completes. You can include a variety of search tokens pertaining to asset search, cloud metadata search and others. All 3 action types (Email, Slack, PagerDuty) support the use of tokens.

Note that only tokens that help in asset scoping or those that are directly related to the alert evaluation are supported for alert rule creation. For instance, the ${action} search token is only applicable if you have a rule that is configured to raise an alert for a remediation action performed in your environment.

When a condition matching the rule is detected, the alert that is generated will include the asset host name, event time, event type, etc. depending on the tokens inserted in the message body.

Monitor Alert Activity



- View all alert activity for the selected timeframe
- Search for alerts using our search tokens, filter to group the alerts by rule name, action name, email recipients, and status

Activity tab lists all the alert activity for the selected timeframe. Here you will see for each alert, rule name, success or failure in sending the alert message, aggregate enabled (Yes) or disabled (No) for the rule, action chosen for the rule, matches found for the rule and the user who created the rule.

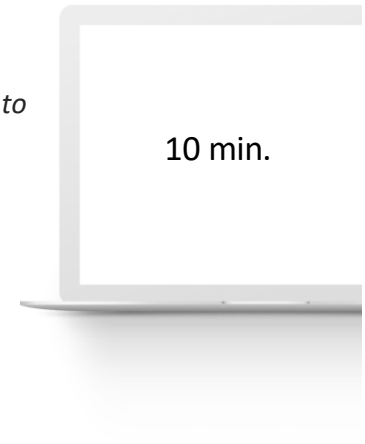
Here you can search for alerts using our search tokens, select a period to view the rules triggered during that time frame, click any bar to jump to the alerts triggered in a certain timeframe and use these filters to group the alerts by rule name, action name, email recipients and status.

LAB 5

Configure Rule Based Alerts

PLAY

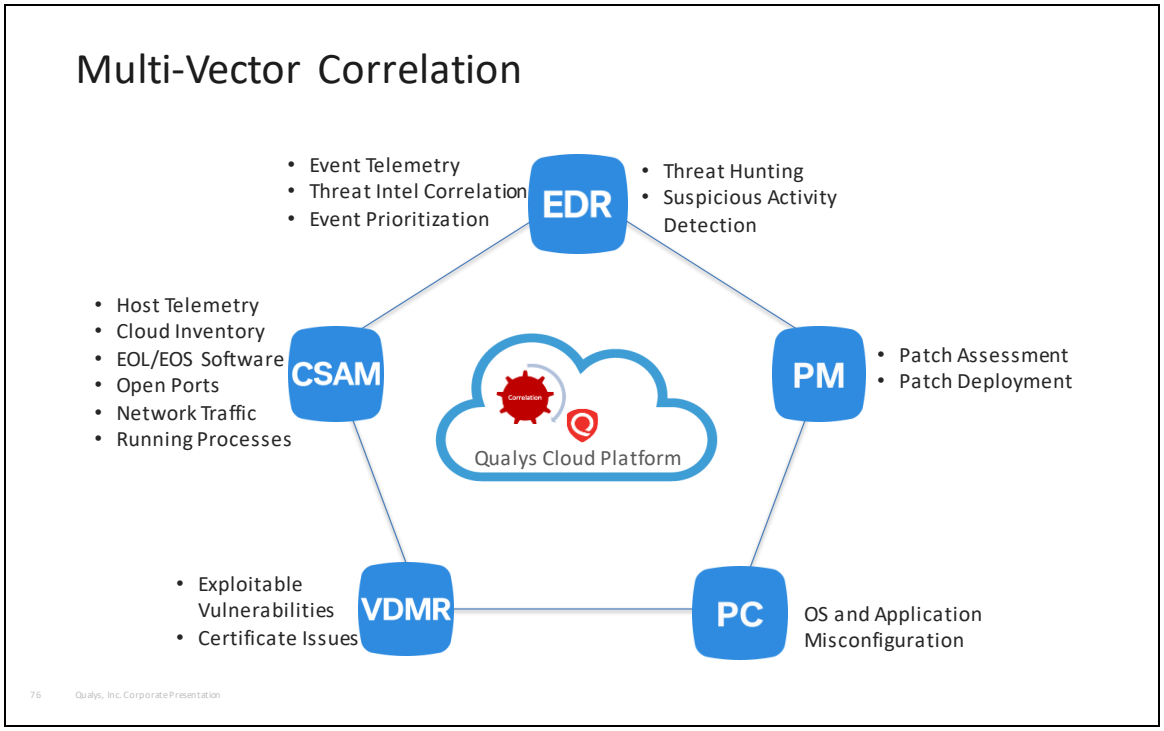
*Please consult **page 19** in the Lab Tutorial Supplement for instructions to perform this lab activity.*



Respond and Prevent

Correlate Prevention across Multiple Vectors

In this section, we will discuss how EDR works with other Qualys applications such as AI, VMDR, PC and PM to correlate multiple attack vectors and provide better context for remediation and prevention.



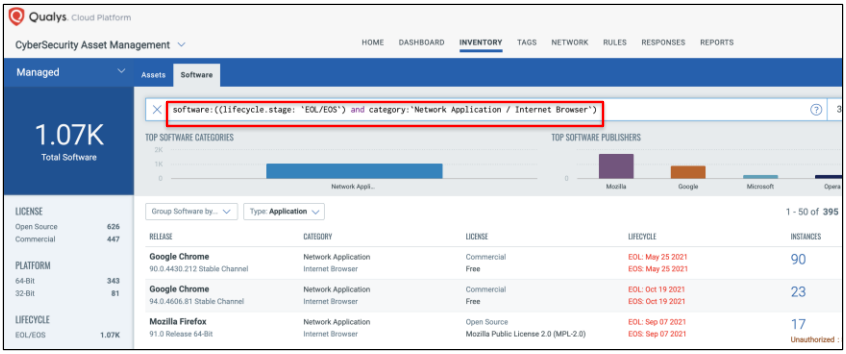
Any cyber attack, large or small is born from a weak link in the security chain.

These weak links take many forms: poorly configured endpoints or network, vulnerable-but-common applications like Microsoft Office, Adobe Reader and Java, EOS platform or software, missing security patches, etc., are common examples.

Multi-vector attacks take advantage of these common vulnerabilities: combining elements like social engineering and 'spear phishing' e-mail messages with malicious attachments that contains code that exploits known or unknown (zero-day) vulnerabilities on the target system. While these attacks might rely on commodity malware, they are often tailored to bypass most antivirus engines.

Qualys EDR creates a Single View of the Asset, showing threat hunting details unified with other Qualys Cloud Apps for hardware and software inventory, vulnerability posture, policy compliance controls, and file integrity monitoring change alerts for on-premise servers, cloud instances, and off-net remote endpoints.
A single user interface significantly reduces the time required for incident responders and security analysts to hunt, investigate, detect, and respond to threats before breach or compromise can occur.

Identify Assets with EOL/EOS Software



- Use queries to quickly identify EOL or EOS software
- Enable EDR on target assets to monitor activity and prevent threats from spreading

77 Qualys, Inc. Corporate Presentation

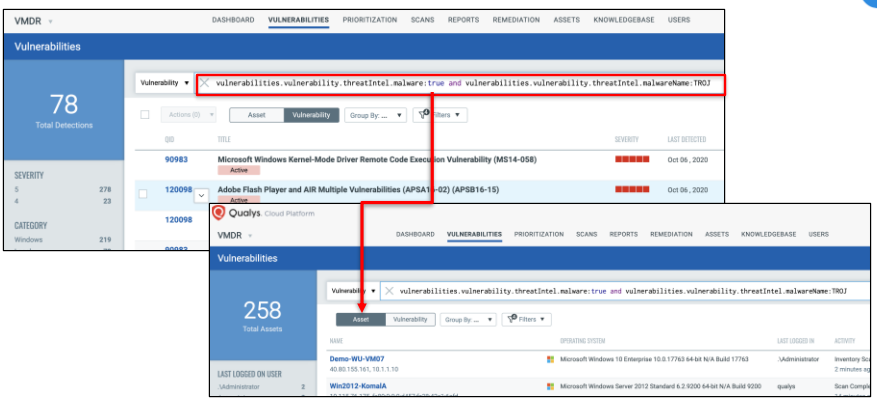
Visibility into software inventory is important to secure assets with end-of-life or EOL and end-of-support or EOS software\browsers.

Qualys CSAM provides the necessary visibility into the asset and software inventory and EDR can monitor activity on such assets and allow timely response to contain or eradicate threats and prevent any breach\compromise from spreading across the enterprise infrastructure.

The following query identifies Windows assets with EOL or EOS software:
operatingSystem:windows and software: (lifecycle.stage:EOL/EOS)

You can run this query under the Software tab in the Inventory section in the CSAM app. Then you can switch to the Assets tab to view all assets that have EOS software\browsers.

Identify Vulnerable Assets



- Use VMDR to quickly identify vulnerabilities associated with specific malware categories detected by EDR
- Identify assets with these vulnerabilities

With combination fo VMDR, Patch Management (PM) and EDR you can eliminate the root-cause of malicious attacks for exploitable vulnerabilities.

Research shows that most breaches happen because of the presence of known exploitable vulnerabilities in the environment. By identifying and remediating such vulnerabilities, you can vastly reduce the chances of a breach in your environment.

Example Scenario:
You have detected incidents related to Malware Category “TROJAN” in your environment and you are tasked with identifying and eliminating the root-cause of this issue. This way you can reduce the chances of more incidents pertaining to the same malware cropping up in your environment.

Solution:
In the hunting tab you can see Incidents related to malware family containing TROJAN present in the environment.

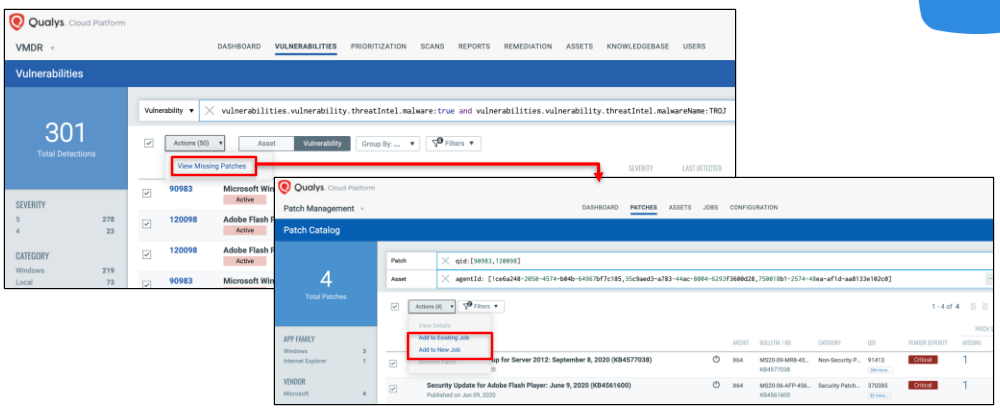
Navigating to the VMDR app, Vulnerabilities tab we can run this query to easily find out all vulnerabilities linked the malware category TROJAN.
vulnerabilities.vulnerability.threatIntel.malware:TRUE and vulnerabilities.vulnerability.threatIntel.malwareName:TROJ

Here you can see all corresponding vulnerabilities in your environment. From here, you can switch to the Assets tab to see all assets which have exploitable vulnerabilities mapped to malware for malware type TROJAN.

The next step is to identify and apply any missing patches that will address these exploitable vulnerabilities.

Identify and Apply Missing Patches

PM



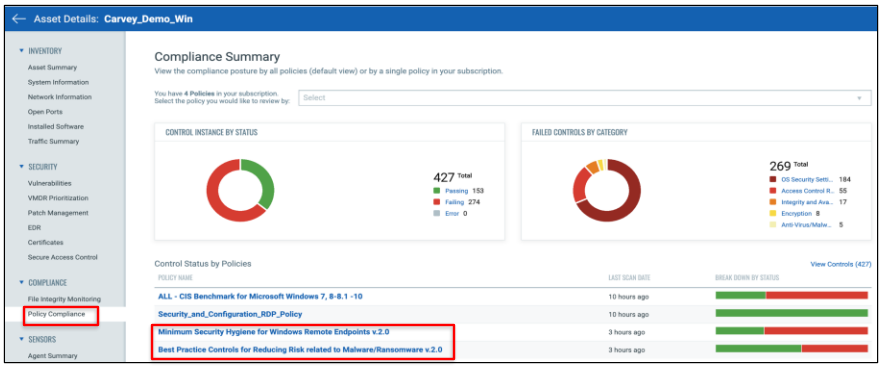
- Quickly identify missing patches and address vulnerabilities associated with different threats using VMDR's integrated workflow for Patch Management
- Eliminate root cause and prevent malware from reinfecting assets

You can quickly find out all missing patches for these exploitable vulnerabilities and then using VMDR's integrated workflows for Patch Management, you can create a patch job to patch all such vulnerabilities across the environment, which otherwise could have been exploited and your team would need to put in time to detect, investigate, again correlate and respond to such incidents.

This approach illustrated here can be used for addressing issues pertaining to any other types of malware categories too.

Additional Context from Configuration Management

PC



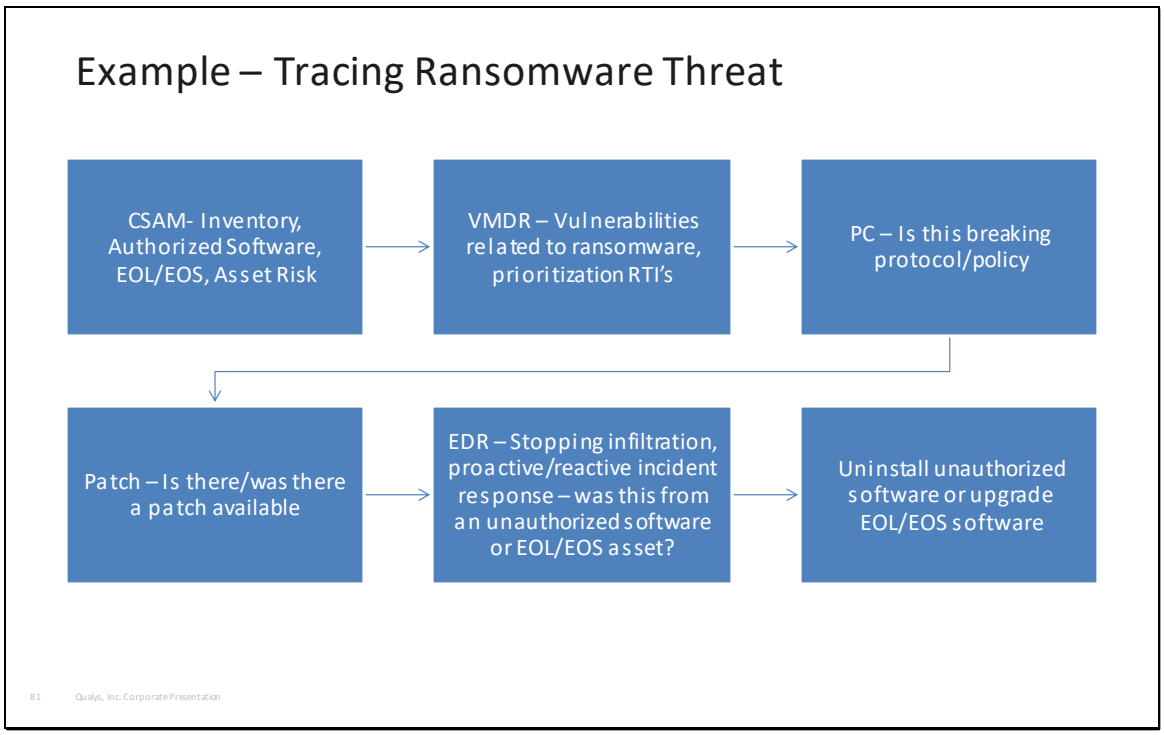
- Identify misconfigurations and improper security controls
- Leverage out of box policies provided by Qualys for control evaluation
- Evaluate compliance posture and reduce risk related to malware\ransomware

In addition to vulnerabilities, an adversary may identify and exploit weaknesses in the configuration of your infrastructure. These weaknesses could include architectural flaws, misconfigurations, or improper security controls.

Searching for failing controls mapped to spread of malware/ransomware or controls mapped to MITRE technique may help identify such misconfigurations and reduce the attack surface.

For example, the Local Security Authority Subsystem Service (LSASS) control failing means you have exploitable misconfigurations that could result in a credential dumping attack. Credential Dumping refers to a variety of methods that adversaries and professional penetration testers use to obtain legitimate usernames and passwords. Legitimate credentials offer adversaries one of the most effective and discreet means of accessing valuable data and systems. Credential Dumping enables initial access, lateral movement, and privilege escalation.

The “Best Practice Controls for Reducing Risk related to Malware/Ransomware” security and compliance policy is provided by Qualys to help organizations in reducing risk of malware and ransomware attacks on a Windows system. The controls within this policy are configured based on the industry recommendations, best practices, standards and guidelines, such as CIS and DISA.


Example – Tracing Ransomware Threat
CSAM- Inventory, Authorized Software, EOL/EOS, Asset Risk
VMDR – Vulnerabilities related to ransomware, prioritization RTI's
PC – Is this breaking protocol/policy
Patch – Is there/was there a patch available
EDR – Stopping infiltration, proactive/reactive incident response – was this from an unauthorized software or EOL/EOS asset?
Uninstall unauthorized software or upgrade EOL/EOS software
81
Qualys, Inc. Corporate Presentation

Ransomware attacks are among the most significant cyber threats facing businesses today. Ransomware attacks are becoming even more sophisticated and massive via the ransomware-as-a-service operating model.

A unified view into critical ransomware exposures such as internet-facing vulnerabilities and misconfigurations, insecure RDP, and detection of risky software in the datacenter environment along with alerting for assets missing anti-malware solutions can play a crucial role in the fight against ransomware attacks.

Assets hosting database systems or critical enterprise applications should be monitored to ensure they are free of unauthorized and EOL/EOS software as this too is a common vector used in such attacks. You should ensure antivirus and anti-malware software are installed and running across an organization's environment to eliminate security tooling blind spots. Qualys CSAM provides you all this visibility in one place.

With VMDR, you can identify Ransomware-specific vulnerabilities which is the most common attack vector used for such attacks.

Another critical attack vector is misconfigurations such as insecure RDP and admin shares that have been leveraged in multiple ransomware attacks. Qualys Policy Compliance can scan for misconfigurations mapped to the relevant MITRE ATTACK

techniques related to Ransomware attacks.

Also, organizations need to urgently prioritize patches for vulnerabilities linked to ransomware attacks, especially on internet-facing assets that are an attacker's first target and patching critical infrastructure assets hosting critical database systems to reduce the attack surface. Using the Qualys Patch Management solution, organizations can accelerate remediation of ransomware exposures with zero-touch patching by continuously patching ransomware vulnerabilities as they are detected. The remediation plan also enables proactive patching for prioritized software to keep software up to date.

And lastly, EDR can help you identify and respond to threats that went undetected through other defenses in your environment. With a "look back" investigation capability in EDR, you can drill-down into the chain of events and identify the root cause and can plug any unaddressed security gaps that still exist in your environment.

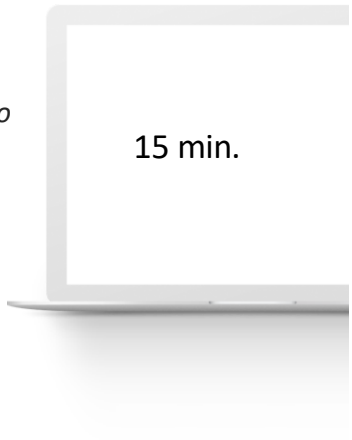
So Qualys solutions namely, CSAM, VMDR, Patch Management and EDR can together provide you that unified view to detect and remediate ransomware threats quickly and easily.

LAB 6

Correlate Prevention Across Multiple Vectors

PLAY

*Please consult **pages 20-23** in the Lab Tutorial Supplement for instructions to perform this lab activity.*



Last Reminders

Certification Exam

30 multiple choice questions.

Answer 75% of the questions correctly to receive a passing score.

Candidates will receive 5 attempts to pass the exam.

You may use the Container Security Assessment Response presentation slides and lab tutorial supplement to help you answer the exam questions.

Trial Account

https://www.qualys.com/free-trial/

Training Survey

https://forms.office.com/r/rsy0Aja6Xz

See the bottom of Swapcard session for the 3 links mentioned above.

The certification exam is open book and is based on multiple choice questions. You need answer at least 75% of the 30 questions right in order to be certified on this course.

We recommend that you take this certification exam at the earliest possible convenience.

Please consult the Lab Tutorial Supplement for information regarding exam registration link.

Also if you want to try our solution, you can submit a request for a free Qualys limited trial account using the link shown on screen.

We value your feedback and so request you to take few minutes of your time to tell us how we did on this particular course using the training survey link.



Thank You

training@qualys.com